



IT Security

Bachelor of Science

Modulhandbuch

Version 1.3

gemäß Studien- und Prüfungsordnung 17.2

Inhalt

| | |
|--|-----------|
| Semester 1 | 4 |
| 11000 Mathematik 1 | 5 |
| 11500 Einführung Informatik | 8 |
| 12000 Programmierung 1 | 11 |
| 12500 Einführung IT Security | 14 |
| 13000 Einführung offensive Security-Methoden | 17 |
| 13500 Digitale Logik | 20 |
| Semester 2 | 23 |
| 14000 Mathematik 2 | 24 |
| 14500 Programmierung 2 | 26 |
| 15000 Betriebssysteme | 29 |
| 15900 Kryptologie 1 | 33 |
| 16500 Formale Grundlagen | 37 |
| 16600 Web-Anwendungen 1 | 40 |
| Semester 3 | 43 |
| 21000 Sichere Datenbanken | 44 |
| 15500 Algorithmik | 49 |
| 21100 Betriebswirtschaftslehre und Management | 52 |
| 21200 Netzwerke | 55 |
| 21300 Rechnertechnik | 59 |
| 21400 Kryptologie 2 | 62 |
| Semester 4 | 65 |
| 22000 Web-Anwendungen 2 | 66 |
| 22100 Wirtschafts- und Internetrecht | 70 |
| 22200 Betriebssicherheit | 73 |
| 22300 Software Engineering | 76 |
| 22500 Reverse Engineering | 79 |
| 22600 Netzwerk- und Systemsicherheit | 82 |
| 22400 Cybersecurity | 86 |
| Semester 5 | 89 |
| 23000 Projektmanagement | 90 |
| 23100 Unternehmenskonzepte / Digitale Fabrik | 93 |
| 23200 Verteilte Systeme (Technik) | 97 |
| 23300 Intelligente Lernende Systeme | 101 |
| 23410 Medieninformatik | 105 |
| 23500 Projektstudium | 109 |
| 23600 Datenbanken 2 | 112 |
| 23700 GUI-Development (Graphical User Interface-Development) | 116 |
| 23800 Softwarearchitektur | 119 |

| | |
|---|------------|
| 23900 Big Data | 123 |
| 24000 IT-Management | 126 |
| 24100 Consulting | 130 |
| 24200 E-Business | 134 |
| 24300 Digitale Forensik | 138 |
| 24400 Offensive Sicherheitsmethoden | 141 |
| Semester 6 | 145 |
| 31000 Integriertes praktisches Studiensemester | 146 |
| 31500 Berufsfertigkeit | 148 |
| Semester 7 | 152 |
| 32000 Simulationstechnik | 153 |
| 32100 Mobile Systeme und Cloud | 157 |
| 32210 Informationsvisualisierung | 161 |
| 32300 IT-GRC (IT-Governance, Risk & Compliance) | 164 |
| 32400 IT-Sicherheitsmanagement | 167 |
| 32500 Mobile und Cloud Forensik | 170 |
| 51000 Bachelor-Thesis | 173 |
| Zuordnung der Module zu Fächergruppen (Säulen) | 176 |
| Informatik | 176 |
| IT Security | 176 |
| Wirtschaftsinformatik | 177 |
| Technische Informatik | 177 |
| Betriebswirtschaftslehre | 178 |
| Fächerübergreifende Qualifikationen | 178 |

Semester 1

| | | | |
|---|---|---|---------------------|
| Modulbezeichnung | 11000 Mathematik 1 | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 11000 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung und Übungen Mathematik 1 | | |
| Studiensemester | 1 | | |
| Modulverantwortliche(r) | Prof. Dr. Andreas Knoblauch | | |
| Dozent(in) | Prof. Dr. Andreas Knoblauch, Prof. Dr. Walter Hower, Prof. Dr. Joachim Gerlach, Prof. Dr. Tobias Häberlein | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 1 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung & Übungen: | 4 SWS, Gruppengröße bis 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 60 h | 90 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | Grundlagen der Mathematik auf dem Niveau der Fachhochschulreife | | |
| Modulziele / Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> kennen die Bedeutung der grundlegenden mathematischen und logischen Begriffe wie Mengen, Funktionen, Relationen, Aussagen, Definitionen, Sätze, Beweise kennen die grundlegenden Begriffe, Strukturen und Sätze der Analysis, wie z.B. Körper, Funktionsklassen, Grenzwerte von Folgen und Reihen, Stetigkeit, Ableitung, Satz von Taylor, Integrale, Trigonometrie kennen die grundlegenden Begriffe und Sätze der Linearen Algebra und Analytischen Geometrie wie z.B. | | |

| | |
|---------------|--|
| | <p>Vektor, Gerade, Ebene, Vektorraum, Lineares Gleichungssystem, lineare Abbildung, Matrix, Determinante, Projektion</p> <p>Fertigkeiten</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können mit reellen und komplexen Zahlen rechnen • können die Lösungen von Gleichungen und Ungleichungen bestimmen • können Grenzwerte von Folgen und Reihen bestimmen • können rationale, trigonometrische, Potenz-, Exponential- und Logarithmus-Funktionen berechnen, ableiten und integrieren • können mit Vektoren und Matrizen rechnen • können lineare Gleichungssysteme aufstellen und lösen • können einfache mathematische Modelle aufstellen und in diesen logisch schlussfolgern • können die Korrektheit von mathematischen Sätzen durch Nachvollziehen von Beweisen beurteilen, und einfache Sätze selbst beweisen <p>Kompetenzen</p> <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben. • Können die Komplexität und Machbarkeit von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen |
| <p>Inhalt</p> | <p>Mathematische Grundlagen:</p> <ul style="list-style-type: none"> • Mengen, Funktionen, Aussagen, Definitionen, Sätze, Beweise <p>Analysis:</p> <ul style="list-style-type: none"> • Körper der reellen und komplexen Zahlen • Funktionen und Funktionsklassen: • Polynome und rationale Funktionen • Potenz-/Wurzel-/Exponential-/Logarithmusfunktionen • Trigonometrische Funktionen • Grenzwerte von Folgen und Reihen • Stetigkeit und Grenzwerte von Funktionen • Differentialrechnung, Ableitungen, Satz von Taylor • Integralrechnung, Integrationstechniken • Funktionen $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$, partielle Differentiation <p>Lineare Algebra und Analytische Geometrie:</p> <ul style="list-style-type: none"> • Geraden und Ebenen |

| | |
|--|--|
| | <ul style="list-style-type: none"> • Vektorrechnung im \mathbb{R}^n • Lineare Gleichungssysteme • Lineare Abbildungen, Matrizen, Determinanten • Koordinatentransformationen, Projektionen • Eigenwerte und Eigenvektoren |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur 90min., benotet |
| Medienformen | Vorlesung mit Beamer, Tafel, Teilskript in PDF-Format über Lernplattform, Übungen an der Tafel |
| Literatur | <p>Teschl G., Teschl S.: „Mathematik für Informatiker - Band 1: Diskrete Mathematik und lineare Algebra“, Springer Verlag</p> <p>Teschl G., Teschl S.: „Mathematik für Informatiker - Band 2: Analysis und Statistik“, Springer Verlag</p> <p>L. Papula: „Mathematik für Ingenieure und Naturwissenschaftler“, mehrbändiges Standardwerk, Vieweg</p> <p>P. Minorski: „Aufgabensammlung der höheren Mathematik“, Fachbuchverlag Leipzig</p> <p>W. Preuß: „Mathematik für Informatiker“, Fachbuchverlag Leipzig</p> <p>M. Kofler, G. Bitsch, M. Komma: „Maple“, Addison-Wesley</p> |

| | | | |
|--------------------------|--|---|---------------------|
| Modulbezeichnung | 11500 Einführung Informatik | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 11500 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung und Übungen Einführung Informatik | | |
| Studiensemester | 1 | | |
| Modulverantwortliche(r) | Prof. Dr. Ute Matecki, Prof. Dr. German Nemirovskij, Prof. Dr. Tobias Häberlein | | |
| Dozent(in) | Prof. Dr. Ute Matecki | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | Technische Informatik, IT-Security, Wirtschaftsinformatik | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 1 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung: | 2 SWS, Gruppengröße bis 60 | |
| | Praktikum: | 2 SWS, Gruppengröße bis 20 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung | 30 h | 45 h |
| | Praktikum | 30 h | 45 h |
| | Summe: 150h <i>(5 * 30 Std./ECTS)</i> | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen | Keine | | |
| Lernziele / Kompetenzen | <p>Kenntnisse</p> <ul style="list-style-type: none"> • Die Studierenden kennen die Grundprinzipien des Aufbaus eines Rechners. • Sie kennen die in der Informatik verwendeten Zahlensysteme und Zeichentabellen und können diese den elementaren Datentypen von C zuordnen. • Sie kennen die wichtigsten Adressierungssysteme und Grundprinzipien von Rechnernetzen. • Sie kennen die wichtigsten Shellbefehle einer ausgewählten Linux-Shell, sowie reguläre Ausdrücke und Umgebungsvariablen. • Sie kennen die wichtigsten Sprachelemente zum Aufbau von Shell-Skripten. | | |

| | |
|--------|--|
| | <ul style="list-style-type: none"> • Sie kennen die Unterschiede zwischen interpretierten und compilierten Programmiersprachen. <p>Fertigkeiten</p> <ul style="list-style-type: none"> • Die Studierenden können Zahlensysteme ineinander umrechnen. • Die Studierenden können mit MAC- und IP-Adressen umgehen und einfache Netzwerkbefehle von der Shell aus ausführen. • Die Studierenden können ein Linux-Betriebssystem von der Shell aus bedienen, sowie einfache Shell-Skripte schreiben. • Sie können interpretierte Programme starten, beispielsweise Bash-Skripte oder Python-Skripte. • Sie können einfache Programme einer compilierten Sprache übersetzen und zum Laufen bringen (beispielsweise C-Programme oder Java-Programme) <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • lernen durch Einführung in praktische Teilgebiete der Informatik in dieser Veranstaltung die Denkweise von Informatikern • sind in der Lage, das Zusammenspiel von Hardware, Betriebssystem und Software einzuordnen. • sind in der Lage, informatische Probleme und Aufgabenstellungen zu erfassen, in Teilprobleme zu zerlegen und eigenständig zu lösen. <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • haben ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um betriebliche Anwendungssysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren. • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • sind in der Lage Systeme sowie Anwendungen zu analysieren, entwerfen, entwickeln und pflegen, sodass sie den heutigen Maßstäben an die Sicherheit gerecht werden |
| Inhalt | <p>Vorlesung</p> <ul style="list-style-type: none"> • Prinzipien Rechneraufbau • Zahlendarstellung, Zeichendarstellung (ASCII-/Unicode-Tabellen) • Prinzipien Rechnernetze, Schichtenmodelle, MAC-Adressen, IP-Adressen |

| | |
|-----------------------------|--|
| | <ul style="list-style-type: none"> • Benutzung eines Betriebssystems am Beispiel Linux: Dateisysteme, Nutzerberechtigungen, Prozesse, einfache Shell-Kommandos, Umgebungsvariablen, reguläre Ausdrücke mit dem grep-Kommando benutzen, Einführung in die Shell-Programmierung mit Variablen und Kontrollstrukturen, Automatisierung einfacher Aufgaben über Shell-Skripte • Unterschied interpretierte Sprachen vs. compilierte Sprachen. <p>Praktikum</p> <ul style="list-style-type: none"> • Umgang mit Zahlensystemen, Adress-Darstellungen, Interpretation von Dateiinhalten • Umgang mit dem Betriebssystem Linux • Shell-Programmierung • Benutzung eines Compilers und eines Interpreters |
| Studien- Prüfungsleistungen | Modul 11505: Klausur, 90 Minuten, benotet Modul 11510: Laborarbeit, unbenotet |
| Medienformen | Vorlesung mit Beamer, Handout in PDF-Format über Lernplattform, Laborübungen und -Testate in einem Labor |
| Literatur | Grundlagen der Informatik, H. Herold et al., Pearson, 2012 Shell-Programmierung. Das umfassende Handbuch, J. Wolf et al., Teubner, 2013 Rechnerarchitektur, A.S. Tanenbaum, Pearson, 2014. Computernetzwerke, A.S. Tanenbaum, Pearson, 2012. |

| | | | |
|--------------------------------------|---|--|--------------|
| Modulbezeichnung | 12000 Programmierung 1 | | |
| ggf. Modulniveau | Grund-Studium | | |
| ggf. Kürzel | 12000 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Programmierung 1 Praktikum Programmierung 1 | | |
| Studiensemester | 1 | | |
| Modulverantwortliche(r) | Prof. Dr. Tobias Häberlein | | |
| Dozent(in) | Prof. Dr. Tobias Häberlein | | |
| Sprache | Deutsch, (deutsches und englisches Literaturstudium erforderlich) | | |
| Zuordnung zum Curriculum | Studiengang: | IT Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflicht | |
| | Semester: | 1 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung: 4 SWS, Gruppengröße bis 150 Praktikum: 2 SWS, Gruppengröße 20 | | |
| Arbeitsaufwand | Veranstaltung/Art | Präsenz | Eigenstudium |
| | Vorlesung & Übungen | 45 h | 75 h |
| | Praktikum | 22,5 h | 82,5 h |
| | Summe: 225h (7,5 * 30 Std./ECTS) | 67,5 h | 157,5 h |
| Kreditpunkte (ECTS) | 7,5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | keine | | |
| Angestrebte Lernergebnisse | Kenntnisse <ul style="list-style-type: none"> 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 Programmierkonstrukte verstanden. | | |

| | |
|---------------|---|
| | <p>Fertigkeiten</p> <ul style="list-style-type: none"> Die Studierenden können imperative, objektorientierte und funktionale Aspekte der Programmiersprache Python zur Lösung von Problemstellungen selbstständig einsetzen und können daraus selbstständig lauffähige wohlstrukturierte Programme entwickeln. <p>Kompetenzen</p> <ul style="list-style-type: none"> 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. 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. Die Studierenden sind in der Lage einfache kleinere Anwendungs- und Softwaresysteme neu zu entwickeln. Durch die verwendete Didaktik in Praktika und Vorlesung werden die Studierenden zu eigenverantwortlichem Handeln, Zeitmanagement und Selbstorganisation angehalten. Durch die Art der Abnahme der im Praktikum erarbeiteten Lösungen werden erste Kompetenzen in Präsentation und Dokumentation erworben. <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei</p> <ul style="list-style-type: none"> INF-1: Absolventen des Studiengangs haben ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um Anwendungs- und Softwaresysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren INF-2: Absolventen des Studiengangs können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen FÜQ-1: Absolventen des Studiengangs können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen |
| <p>Inhalt</p> | <p>Verwendet wird die Programmiersprache Python.</p> <ul style="list-style-type: none"> Grundlagen der Imperativen Programmierung: <ul style="list-style-type: none"> Ausdrücke, Zuweisungen, Schleifen, Bedingungen, Variablen, Funktionen, Einfache Datentypen, Zusammengesetzte Datentypen. Grundlagen der Objekt-Orientierten Programmierung: |

| | |
|--|--|
| | <ul style="list-style-type: none"> ○ Kapselung, Information Hiding, Klassen, Objekte, Methoden Überladung, Vererbung, Exceptions. • Grundlagen der Funktionalen Programmierung: <ul style="list-style-type: none"> ○ Lambda-Ausdrücke, Funktionen höherer Ordnung, map-Funktion, filter-Funktion, reduce-Funktion, enumerate, zip, List Comprehensions, Numerical Python • Sonstiges: <ul style="list-style-type: none"> ○ Entwicklungsumgebungen (Verschiedene Editoren wie emacs, vi, eclipse), Python-Interpreter-Umgebungen, IPython Notebooks, Versionsmanagement-Systeme (git). |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur 120 min, benotet Laborarbeit, unbenotet |
| Medienformen | Vorlesung mit Beamer; Implementierung konkreter Anwendungsfälle und Visualisierung mit Beamer; Übungen und Tests in einem Labor |
| Literatur | Tobias Häberlein: Informatik: Eine praktische Einführung mit Bash und Python (De Gruyter Studium), 2016 Dusty Phillips: Python 3 Object Oriented Programming. Harness the power of Python 3 objects. Packt publishing, 2010. |

| | | | |
|------------------------------------|---|---|--------------|
| Modulbezeichnung | 12500 Einführung IT Security | | |
| ggf. Modulniveau | Grund-Studium | | |
| ggf. Kürzel | 12500 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Einführung IT Security Praktikum Einführung IT Security | | |
| Studiensemester | 1 | | |
| Modulverantwortliche(r) | Prof. Dr. Tobias Heer, Prof. Holger Morgenstern | | |
| Dozent(in) | Prof. Dr. Tobias Heer | | |
| Sprache | Deutsch, (deutsches und englisches Literaturstudium erforderlich) | | |
| Zuordnung zum Curriculum | Studiengang: | IT Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflicht | |
| | Semester: | 1 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung: 4 SWS, Gruppengröße bis 150 | | |
| Arbeitsaufwand | Veranstaltung/Art | Präsenz | Eigenstudium |
| | Vorlesung & Übungen | 60 h | 90 h |
| | Summe: 150h <i>(5 * 30 Std./ECTS)</i> | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen Prüfungsordnung | nach | Keine | |
| Empfohlene Voraussetzungen | keine | | |
| Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • kennen die wichtigsten Konzepte und Technologien aus dem Bereich sicheres Informationsmanagement und -Austausch zwischen vernetzten betrieblichen Anwendungen • kennen die Grundprinzipien der digitalen Verschlüsselung • Kennen Bedrohungen und Risiken für IT Systeme | | |

| | |
|--|--|
| | <ul style="list-style-type: none">• Beispiele für Sicherheitszwischenfälle in der jüngeren Vergangenheit <p>Fertigkeiten</p> <p>Die Studierenden können</p> <ul style="list-style-type: none">• Sicherheitsrisiken einschätzen und bewerten• Die Sicherheit von Verschlüsselungsverfahren einschätzen• Maßnahmen zum Schutz vor Viren und Würmern einschätzen und umsetzen• Einen Internet-fähigen Personal-Computer sicher konfigurieren und betreiben• Angriffe in der Praxis erkennen und einordnen <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none">• sind in der Lage Gefahren bzw. Bedrohungen für die Vertraulichkeit und die Integrität der Information zu identifizieren und die Maßnahmen zu beschreiben, welche den oben genannten Bedrohungen effektiv entgegengesetzt werden• sind in der Lage ein bereits bestehendes IKT-Sicherheitskonzept zu verstehen, zu testen und zu verbessern• sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl von geeigneten Sicherheitstechniken befähigt• sind in der Lage Systeme zu analysieren und auf die heutigen Maßstäbe an die Sicherheit zu untersuchen• sind sich ihrer Verantwortung gegenüber Individuen und der Gesellschaft beim Umgang mit Sicherheitsrelevanten Informationen und Sicherheitsmethoden bewusst <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none">• haben ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um betriebliche Anwendungssysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren• können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen• können sich und die Wirkung ihrer Person auf andere einschätzen und beweisen sich durch ihre adäquaten Mitarbeiterqualifikationen; beherrschen eine kooperative Teamarbeit in der sie Verantwortung tragen können und auch in widersprüchlichen Situationen tragfähige Entscheidungen treffen können |
|--|--|

| | |
|--|--|
| | <ul style="list-style-type: none"> • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams |
| Inhalt | <p>Vorlesung & Übungen</p> <p>Ziele und Begriffe der Informationssicherheit</p> <ul style="list-style-type: none"> • Grundlegende Begriffe der Informationssicherheit • Schutzziele, Schwachstellen, Bedrohungen, Angriffe • Angriffs- und Angreifertypen • Risikobetrachtung, Risikobewertung und Handlungsalternativen • Aktuelle Entwicklungen Bedrohungslage, Maßnahmen, Kosten, Arbeitsmarkt • Incident 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 <p>Datensicherung, Datenwiederherstellung und Datenlöschung im Überblick</p> |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur 90 min, benotet |
| Medienformen | Vorlesung mit Beamer; Implementierung konkreter Anwendungsfälle und Visualisierung mit Beamer; Übungen und Tests in einem Labor |
| Literatur | <p>Schmeh, K.: Kryptografie, dpunkt Verlag, 5. Auflage, Wiley, 2013</p> <p>Biskup, J.: Security in Computing Systems, Springer, 2010</p> <p>Schwenk, J.: Sicherheit und Kryptographie im Internet, Springer, 2014</p> <p>Kappes, M.: Netzwerk- und Datensicherheit, Springer, 2013</p> <p>Eckert, C.: IT-Sicherheit, 9. Auflage, Oldenbourg Wissenschaftsverlag, München, 2014</p> |

| | | | |
|---|--|----------------------------|---------------------|
| Modulbezeichnung | 13000 Einführung offensive Security-Methoden | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 13000 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung Einführung offensive Security-Methoden, Seminar Einführung offensive Security-Methoden | | |
| Studiensemester | 1 | | |
| Modulverantwortliche(r) | Prof. Dr. Tobias Heer | | |
| Dozent(in) | Prof. Dr. Tobias Heer | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 1 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung & Seminar: | 2 SWS, Gruppengröße bis 75 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Seminar | 30 h | 45 h |
| | Summe: 75h (2,5 * 30 Std./ECTS) | 30 h | 45 h |
| Kreditpunkte (ECTS) | 2,5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | Keine | | |
| Modulziele / Angestrebte Lernergebnisse | Kenntnisse Die Studierenden <ul style="list-style-type: none"> • kennen die Ziele und Grenzen von Penetrationstests • kennen die Methodik und Ablauf eines Penetrationstests • sind sich über praktische, zwischenmenschliche und rechtliche Problemfelder beim Einsatz von offensiven Security Methoden bewusst • kennen Techniken zur Informationsbeschaffung über Zielsysteme • kennen verschiedene offensive Techniken • kennen die moralischen und rechtlichen Grenzen beim Einsatz offensiver Methoden | | |

| | |
|---------------|---|
| | <p>Fertigkeiten</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können die vorbereitenden Schritte eines Penetrationstests anwenden • können ausgewählte offensive Techniken anwenden <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind dazu befähigt, betriebliche Informations- und Anwendungssysteme samt ihrer Komponenten zu analysieren und zu entwerfen. Einen besonderen Schwerpunkt stellen dabei ERP Systeme im betrieblichen Kontext dar • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind dazu befähigt, Daten und Prozessmodelle mit gängigen Modellierungsmethoden zu entwerfen, zu analysieren und Heuristiken für die Optimierung anzuwenden • können sich und die Wirkung ihrer Person auf andere einschätzen und beweisen sich durch ihre adäquaten Mitarbeiterqualifikationen; beherrschen eine kooperative Teamarbeit in der sie Verantwortung tragen können und auch in widersprüchlichen Situationen tragfähige Entscheidungen treffen können • sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt • 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 • sind sich ihrer Verantwortung gegenüber Individuen und der Gesellschaft beim Umgang mit Sicherheitsrelevanten Informationen und Sicherheitsmethoden bewusst |
| <p>Inhalt</p> | <p>Vorlesung & Seminar</p> <ul style="list-style-type: none"> • Motivation offensiver Sicherheitsmethoden • Rechtliche und moralische Grundlagen |

| | |
|--|---|
| | <ul style="list-style-type: none"> • Ablauf von Penetrationstests (Testvorbereitung, Informationsbeschaffung, Zielanalyse, Angriff, Dokumentation und Abschlussgespräch) <p>Referate zu Themen wie:</p> <ul style="list-style-type: none"> • 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 |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Referat (15 min), benotet |
| Medienformen | Vorlesung mit Beamer, Tafel, Skript digital (über Lernplattform) |
| Literatur | <p>Institute for Security and Ipen Methodologies, Open Source Security Testing Methodology Manual (OSSTM) Online: www.isecom.org/osstmm/</p> <p>C. Hadnagy, Social Engineering: The Art of Human Hacking</p> <p>Wechselnde Online-Literatur für den Referatsteil</p> |

| | | | |
|--------------------------------------|--|----------------|--------------|
| Modulbezeichnung | 13500 Digitale Logik | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 13500 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Digitale Logik | | |
| Studiensemester | 1 | | |
| Modulverantwortliche(r) | Prof. Dr. Joachim Gerlach | | |
| Dozent(in) | Prof. Dr. Joachim Gerlach | | |
| Sprache | Deutsch, (deutsches und englisches Literaturstudium erforderlich) | | |
| Zuordnung zum Curriculum | Studiengang: | IT Security | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflicht | |
| | Semester: | 1 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung: 4 SWS, Gruppengröße bis 150 | | |
| Arbeitsaufwand | Veranstaltung/Art | Präsenz | Eigenstudium |
| | Vorlesung & Übungen | 60 h | 90 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | keine | | |
| Empfohlene Voraussetzungen | keine | | |
| Angestrebte Lernergebnisse | <p>Vermittlung von Kenntnissen bzgl. 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.</p> <p>Kenntnisse</p> <p>Die Studierenden kennen</p> <ul style="list-style-type: none"> das grundlegende Vorgehen zur binären Darstellung von Information in digitalen Rechnersystemen | | |

| | |
|--------|--|
| | <ul style="list-style-type: none"> • grundlegende Vorgehensweisen zur Umsetzung von funktionalem Verhalten in eine schaltungstechnische Realisierung <p>Fertigkeiten</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> • Schaltnetze und Schaltwerke entwerfen, optimieren, und in eine schaltungstechnische Realisierung überführen <p>Kompetenzen</p> <p>Die Studierenden sind in der Lage</p> <ul style="list-style-type: none"> • eine gegebene Problemstellung systematisch in eine für die digitale Verarbeitung geeignete Form zu überführen und in eine digitale Schaltung abzubilden • beim Schaltungsentwurf unterschiedliche Optimierungsziele, etwa Geschwindigkeit, Komplexität, Sicherheit und Zuverlässigkeit, zu berücksichtigen <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben • 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 |
| Inhalt | <p>Vorlesung:</p> <p>Teil-1: Einführung in Digitale Rechnersysteme</p> <ul style="list-style-type: none"> • Einleitung • Vom Abakus zum Supercomputer <p>Teil-2: Grundlagen der Digitalen Datenverarbeitung</p> <ul style="list-style-type: none"> • Grundlagen der Digitaltechnik • Zahlendarstellung und Codes • Boolesche Algebra <p>Teil-3: Digitale Schaltungstechnik</p> <ul style="list-style-type: none"> • Kombinatorische Schaltungen |

| | |
|--|---|
| | <ul style="list-style-type: none"> • Sequentielle Schaltungen • Entwurf digitaler Schaltungen heute |
| Studien-/Prüfungsleistungen/ Prüfungsformen | <ul style="list-style-type: none"> • Klausur 90 Min, Benotet |
| Medienformen | Vorlesung: PC mit Beamer, Folienskript, Tafelanschrieb |
| Literatur | <p>Hoffmann D.W.: Grundlagen der Technischen Informatik. Carl Hanser Verlag.</p> <p>Fricke K.: Digitaltechnik. Vieweg+Teubner Verlag.</p> <p>Siemers C., Sikora A.: Taschenbuch Digitaltechnik. Carl Hanser Verlag.</p> |



Semester 2

| | | | |
|---|--|---|---------------------|
| Modulbezeichnung | 14000 Mathematik 2 | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 14000 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Mathematik 2, Vorlesung und Übungen | | |
| Studiensemester | 2 | | |
| Modulverantwortliche(r) | Prof. Dr. Walter Hower | | |
| Dozent(in) | Prof. Dr. Walter Hower, Prof. Dr. Andreas Knoblauch, Prof. Dr. Joachim Gerlach | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 2 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung & Übungen: | 4 SWS, Gruppengröße 150 | |
| | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 60 h | 90 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 11000 Mathematik 1 Die Studierenden kennen <ul style="list-style-type: none"> • Aussagen, Definitionen, Sätze, Beweise • Körper, Folgen und Reihen-Grenzwerte, Stetigkeit, Ableitung, Satz von Taylor, Integrale, Trigonometrie • Gerade, Ebene, Vektorraum, Lineares Gleichungssystem, Matrix | | |
| Modulziele / Angestrebte Lernergebnisse | Kenntnisse Die Studierenden kennen <ul style="list-style-type: none"> • Grundlagen der Mathematik für Informatiker | | |

| | |
|--|--|
| | <p>Fertigkeiten</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> • mathematische Sachverhalte formalisieren • Zähl-Probleme systematisch angehen und lösen <p>Kompetenzen</p> <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse bei:</p> <p>Die Studierenden sind fähig,</p> <ul style="list-style-type: none"> • komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben. |
| Inhalt | <p>Vorlesung & Übungen</p> <ul style="list-style-type: none"> • Fundamentales <ul style="list-style-type: none"> ○ Natürliche Zahlen ○ Funktionen ○ Relationen • Mengen <ul style="list-style-type: none"> ○ Operationen ○ Endliche Mengen ○ Abzählbarkeit und Überabzählbarkeit • Kombinatorik <ul style="list-style-type: none"> ○ Grundlegende Zähl-Techniken ○ Ein-/Ausschluss ○ Rekurrenz-Relation ○ Fakultät, Permutation ○ Binomialkoeffizient, Binom.-Satz, Kombination ○ Permutations-Koeffizient, Variation ○ Stirling-Zahlen 1. und 2. Art, Bell-Zahlen • Zahlen-Theorie <ul style="list-style-type: none"> ○ modulare Arithmetik ○ Primfaktor-Zerlegung • Wahrscheinlichkeits-Rechnung <ul style="list-style-type: none"> ○ allgemein ○ bedingt ○ Dichte, Verteilung, Erwartungswert, Varianz |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur 90 min., benotet |
| Medienformen | Folien-Skript, Beamer-PPT, Tafel-Aktionen |
| Literatur | <p>Walter Hower: Diskrete Mathematik – Grundlage der Informatik; Oldenbourg Wissenschaftsverlag, 2010, 978-3-486-58627-5, De Gruyter, 2011, 978-3-486-71164-6.</p> <p>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.</p> <p>A. Arnold, I. Guessarian: Mathématiques pour l’informatique, 4^e édition, Dunod, 2005, 978-2-100-49230-5</p> <p>J. Buchmann: Einführung in die Kryptographie; 5. Auflage, Springer, 2010, 978-3-642-11185-3.</p> |

| | | | |
|--------------------------------------|--|------------------------------------|---------------------|
| Modulbezeichnung | 14500 Programmierung 2 | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 14500 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung und Übungen Programmierung 2 Praktikum Programmierung 2 | | |
| Studiensemester | 2 | | |
| Modulverantwortliche(r) | Prof. Dr. G. Nemirovski, Prof. Dr. U. Matecki, Prof. Dr. T. Eppler | | |
| Dozent(in) | Prof. Dr. G. Nemirovski, Prof. Dr. U. Matecki, Prof. Dr. T. Eppler | | |
| Sprache | Deutsch, bei Bedarf Englisch (muss vor Semesterbeginn geäußert werden) | | |
| Zuordnung zum Curriculum | Studiengang: | IT Security, Technische Informatik | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 2 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung & Übungen: | 4 SWS, Gruppengröße 150 | |
| | Praktikum: | 2 SWS, Gruppengröße 20 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen: | 60 h | 50 h |
| | Praktikum: | 30 h | 85 h |
| | Summe: 225 h (7,5 * 30 Std./ECTS) | 90 h | 135 h |
| Kreditpunkte (ECTS) | 7,5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | Kenntnisse auf dem Bereich der Software-Entwicklung, konkret Module: <ul style="list-style-type: none"> • 11500 Einführung Informatik • 12000 Programmieren 1 | | |
| Angestrebte Lernergebnisse | Kenntnisse Die Studierenden kennen <ul style="list-style-type: none"> • die prozeduralen Programmier Techniken auf Basis der Programmiersprachen Java und C/C++ | | |

| | |
|--|---|
| | <ul style="list-style-type: none"> • die Paradigmen des objektorientierten Entwurfs sowie des objektorientierten Programmierens auf Basis der Programmiersprachen Java und C/C++ • die grundlegenden Darstellungsmethoden für den objektorientierten Entwurf nach UML (Klassendiagramme) <p>Fertigkeiten</p> <p>Die Studierenden sind in der Lage</p> <ul style="list-style-type: none"> • gegebene Aufgabenstellungen aus dem Bereich der IT-Security und der Technischen Informatik als Java- bzw. C/C++ Programme zu konzipieren und abzubilden • einen objektorientierten Entwurf zu komplexen Themenstellungen zu erstellen und als Java- bzw. C/C++ Anwendung zu implementieren • generische Programmelemente in Java bzw. C/C++ zu entwerfen und zu implementieren • Datenlese- und -schreiboperationen in Java bzw. C/C++ zu implementieren <p>Kompetenzen</p> <p>Die Studierenden sind fähig</p> <ul style="list-style-type: none"> • komplexe Zusammenhänge der Aufgabenstellung in einem objektorientierten Entwurf abzubilden • komplexe Java- und C/C++ Programme zu implementieren • objektorientierte Entwürfe zu gegebenen Aufgabenstellungen zu erstellen • komplexe Programmsysteme zu entwerfen und als Java- oder C/C++ Programme zu implementieren • die unterschiedlichen objektorientierten Eigenschaften der Programmiersprachen C++, Java und Python zu bewerten und anzuwenden <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • haben ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um betriebliche Anwendungssysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren • können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen • Sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben |
|--|---|

| | |
|--|---|
| | <ul style="list-style-type: none"> • 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 • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams |
| <p>Inhalt</p> | <p>Vorlesung, Übungen und Praktikum</p> <ul style="list-style-type: none"> • 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++ • Programmieren im Großen: Definition von Paketen • Das Vererbungskonzept in Java bzw. C++ • Exception Handling • Schnittstellen • Generische Einheiten • Dateien und Streams |
| <p>Studien-/Prüfungsleistungen/ Prüfungsformen</p> | <p>Klausur 120 min, benotet Praktische Arbeit, unbenotet</p> |
| <p>Medienformen</p> | <p>Vorlesung mit Beamer; Skript in PDF-Format; Implementierung konkreter Anwendungsfälle und Visualisierung mit Beamer; Übungen und Tests in einem Labor</p> |
| <p>Literatur</p> | <p>Ullenboom, Chr.: Java ist auch eine Insel, Galileo Computing, 10. Auflage, 2014</p> <p>Goll, J., Heinisch, C.: Java als erste Programmiersprache, Springer Vieweg, 7. Auflage, 2014</p> <p>Krüger, G., Hansen, H.: Java-Programmierung – Das Handbuch zu Java 8, O'Reilly Köln, 8. Auflage 2014</p> <p>http://docs.oracle.com/javase/tutorial/</p> <p>http://www.oracle.com/technetwork/java/api-141528.html</p> <p>http://docs.oracle.com/javase/8/docs/api/</p> <p>https://www.java.com/</p> <p>https://www.uni-trier.de/fileadmin/urt/doku/java/v80/java8.pdf</p> <p>ANSI C, Grundlagen der Programmierung, Herdt-Verlag, 2013</p> <p>ANSI C++, Grundlagen der Programmierung, Herdt-Verlag, 2011</p> |

| | | | |
|--------------------------------------|---|------------------------------------|---------------------|
| Modulbezeichnung | 15000 Betriebssysteme | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 15000 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | 15005 Vorlesung Betriebssysteme 15010 Praktikum Betriebssysteme | | |
| Studiensemester | 2 | | |
| Modulverantwortliche(r) | Prof. Dr. Martin Rieger | | |
| Dozent(in) | Prof. Dr. Martin Rieger | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | Technische Informatik, IT-Security | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflicht | |
| | Semester: | 2 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung: 3 SWS, Gruppengröße bis 150 Praktikum: 1 SWS, Gruppengröße bis 20 | | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 45 h | 45 h |
| | Praktikum | 15 h | 45 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 11500 Einführung Informatik Kenntnisse in C-Programmierung | | |
| Angestrebte Lernergebnisse | Kenntnisse Die Studierenden kennen Die Studierenden kennen <ul style="list-style-type: none"> • Architektur, Konzepte und Mechanismen in Betriebssystemen | | |

| | |
|--|---|
| | <ul style="list-style-type: none"> • Sicherheitskonzepte in Betriebssystemen • Konzepte der Systemprogrammierung in Unix und Windows • Aufbau von I/O-Geräten • Die wichtigsten Dateisysteme <p>Fertigkeiten</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> • Einfache Analyse von Arbeitsplatzrechnern • Administration von Windows-Rechnern • Administration von Unix-Rechnern • Einfache Sicherheits-Policies umsetzen • Systemprogramm zum Umgang mit Dateien und Prozessen entwerfen und erstellen • Systemprogramm für Client-Server-Anwendungen entwerfen und erstellen • Einige Eigenschaften von Dateisystemen analysieren <p>Kompetenzen</p> <p>Die Studierenden sind fähig</p> <ul style="list-style-type: none"> • sind fähig die Begriffe im Bereich Betriebssysteme zu verstehen und aktiv anzuwenden • sind fähig Betriebssysteme anhand wichtiger Merkmale zu beurteilen • sind in der Lage die Betriebssysteme Unix und Windows mit Mitteln der Systemprogrammierung nutzen • sind dazu fähig, Mechanismen zur Prozess-, Speicher- I/O-Verwaltung verstehen <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • verfügen über die zur Erfüllung von Anforderungen der Berufspraxis notwendigen persönlichen Kompetenzen: eigen-verantwortliches Handeln, Zeitmanagement, Selbstorganisation • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben • sind dazu befähigt, Daten und Prozessmodelle mit Mitteln des Betriebssystems zu entwerfen, zu analysieren und zu optimieren • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt • sind in der Lage Systeme sowie Anwendungen zu analysieren, entwerfen, entwickeln und pflegen, sodass sie den heutigen Maßstäben an die Sicherheit gerecht werden |
|--|---|

| | |
|--------|---|
| | <ul style="list-style-type: none"> • 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 • 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 • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams |
| Inhalt | <ul style="list-style-type: none"> • Begriffe und Konzepte <ul style="list-style-type: none"> ○ Begriffe und Konzepte von Betriebssystemen ○ Strukturen von Betriebssystemen ○ Unix/Linux: Benutzerverwaltung, Dateien, Verzeichnisse und das Dateisystem, Zugriffsrechte, Zugriffskontrolle, ○ Logdateien, Kommandozeileninterpreter (Shell) • MS Windows Betriebssystem <ul style="list-style-type: none"> ○ Grundlegende Konzepte und Begriffe, Zugang zu Windows mit „Bordwerkzeugen“, Leistungsüberwachung, ○ System Architektur, wichtige Komponenten der Windows Architektur, ○ Sicherheits-Komponenten, Integritätsstufen und mandatorische Zugriffsregeln, Sicherheitsdeskriptoren und diskrete Zugriffskontrolllisten (DACL), Zugriffskontrolle auf Objekte, Benutzerrechte und Privilegien • Systemprogrammierung in PowerShell <ul style="list-style-type: none"> ○ Sprachkonzept ○ Zugriff auf Systemressourcen ○ Systemprogrammierung in Beispielen • System und Systemprogrammierung in Unix: <ul style="list-style-type: none"> ○ Dateien, Prozesse, Signale, Message Queues, Semaphore, Sockets. ○ Verallgemeinerung und Vertiefung zu Prozessen; • Implementierungen von Prozessen und Scheduling bei Unix und MS Windows; • Speicherverwaltung: Verallgemeinerung und Vertiefung zu Speicherverwaltung; Implementierungen der Speicherverwaltung bei Unix und MS Windows • Eingabe und Ausgabe (IO): Geräte, Konzepte und Architektur für IO, Festplatte als Beispiel • Dateisysteme: Konzepte der Datenträgerverwaltung; Implementierungen in FAT, NTFS und Ext |

| | |
|--|---|
| Studien-/Prüfungsleistungen/ Prüfungsformen | Modul 15005 Klausur 120 min, benotet Praktikum 15010: Praktische Arbeit, unbenotet |
| Medienformen | Vorlesung mit Beamer; Skript in PDF-Format; Implementierung konkreter Anwendungsfälle und Visualisierung mit Beamer; Übungen und Tests in einem Labor |
| Literatur | <p>Andrew S. Tanenbaum: Moderne Betriebssysteme. München u.a.: Pearson Studium, 2016.</p> <p>Glatz, E.: Betriebssysteme : Grundlagen, Konzepte, Systemprogrammierung. Heidelberg: dpunkt, 2015.</p> <p>Schwichtenberg, H.: Windows PowerShell 5.0. Carl Hanser Verlag GmbH, 2016</p> <p>Kofler, M.: Linux: Das umfassende Handbuch. Rheinwerk Computing; 2015</p> |

| | | | |
|--------------------------------------|--|----------------|--------------|
| Modulbezeichnung | 15900 Kryptologie 1 | | |
| ggf. Modulniveau | Grund-Studium | | |
| ggf. Kürzel | KY-1 | | |
| ggf. Untertitel | Krypto-1 | | |
| ggf. Lehrveranstaltungen | Vorlesung und Übung Mathematische Kryptologie 1 Vorlesung und Übung Angewandte Kryptologie 1 | | |
| Studiensemester | 2 | | |
| Modulverantwortliche(r) | Prof. Dr. Walter Hower, Prof. Dr. Tobias Heer | | |
| Dozent(in) | W. Hower, T. Heer | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflicht | |
| | Semester: | 2 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | 15510 Vorlesung + Übung Mathemat. Kryptologie 1: 2 SWS, Gruppengröße bis 150 15520 Vorlesung + Übung Angewandte Kryptologie 1: 2 SWS, Gruppengröße bis 150 | | |
| Arbeitsaufwand | Veranstaltung/Art | Präsenz | Eigenstudium |
| | 15510 V + Ü. Mathem. Kryptol. 1 | 30 h | 45 h |
| | 15520 V + Ü Angew. Kryptol. 1 | 30 h | 45 h |
| | Summe: 150 h (5 * 30 Std.) / [5 ECTS]) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | Mathematik 1, Einführung IT Security | | |
| Angestrebte Lernergebnisse | Kenntnisse Die Studierenden kennen <ul style="list-style-type: none"> • Zahlen-Systeme • Ring-Strukturen • Grundlagen der Mathematik für Informatiker • Die historische Entwicklung der symmetrischen Kryptografie | | |

| | |
|--|--|
| | <ul style="list-style-type: none"> • Symmetrische und asymmetrische Verschlüsselungsverfahren • Verfahren zum Schutz der Integrität • Verfahren zur Authentifizierung • Hash-Funktionen und deren Limitierungen <p>Fertigkeiten</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> • mathematische Sachverhalte formalisieren • Gesetzmäßigkeiten sinnvoll nutzen • Bijektionen einsetzen • Kryptographische Methoden einordnen und deren inhärenten Stärken und Schwächen verstehen • Angriffe gegen historische Chiffren verstehen und anwenden • die Stärke aktueller kryptografischer Verfahren einschätzen und sinnvolle Verfahren auswählen <p>Kompetenzen</p> <p>Die Studierenden sind fähig</p> <ul style="list-style-type: none"> • den größten gemeins. Teiler 2er Zahlen zu berechnen • Modular-Arithmetik zu betreiben • auf Nicht-Primzahl zu testen • RSA und Diffie Hellman auf kleinen Zahlen nachvollziehen und berechnen • Schlüsselstärken bewerten • die Entropie einer binären Zufallsquelle zu verstehen und berechnen <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt • sind in der Lage Systeme sowie Anwendungen zu analysieren, entwerfen, entwickeln und pflegen, sodass sie den heutigen Maßstäben an die Sicherheit gerecht werden • 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 • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben. |
|--|--|

| | |
|--|--|
| Inhalt | <p>Vorlesung und Übung</p> <ul style="list-style-type: none"> • Unterbau <ul style="list-style-type: none"> ○ Bijektion ○ Komposition ○ Zahlensysteme • Zahlen-Theorie <ul style="list-style-type: none"> ○ Kardinalität ○ Teiler, Euklid'scher GGT-Algorithmus ○ ganzzahlige Division mit Rest-Bildung ○ Ring-Strukturen und Modulare Arithmetik • RSA-Verfahren <ul style="list-style-type: none"> ○ öffentlich-private Schlüssel-Konstruktion ○ per „Einweg“-Funktion verschlüsseln ○ via Exponentiation entschlüsseln • Grundlagen der symmetrischen Verschlüsselung <ul style="list-style-type: none"> ○ Substitution und Transposition ○ Cäsar-, Skytale-, Homophone-, Vigenère-, und Vernam-Verschlüsselung sowie One-Time-Pad ○ Angriffe gegen symmetrische Chiffren • Moderne symmetrische Verschlüsselungsverfahren <ul style="list-style-type: none"> ○ Data Encryption Standard (DES) ○ Advanced Encryption Standard (AES) • Zufallszahlen und Zufallszahlengeneratoren <ul style="list-style-type: none"> ○ Entropie und Zufälligkeit ○ Zufallsquellen ○ Schlüssel und Schlüssellängen • Hash-Funktionen <ul style="list-style-type: none"> ○ Merkle Damgård Verfahren ○ SHA-Familie ○ Stärke und Angriffe auf Hash-Funktionen ○ Kollisionsattacken und das Geburtstagsparadoxon • Angewandte asymmetrische Kryptografie <ul style="list-style-type: none"> ○ Schlüsselaustausch mit RSA und Diffie Hellman ○ RSA Backdoors ○ Digitale Signaturen und Public Key Infrastruktur |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Zwei Klausuren, je 45 min; benotet |
| Medienformen | Skript in PDF-Format; Vorlesung mit Beamer, Übungen an der Tafel |
| Literatur | <ul style="list-style-type: none"> • W. Hoyer: Diskrete Mathematik – Grundlage der Informatik. Oldenbourg Wissenschaftsverlag, 2010, 978-3-486-58627-5 (Papier); De Gruyter, 2011, 978-3-486-71164-6 (eBook) • K. Schmech: Kryptografie. dpunkt.verlag, 2016, 978-3-86490-356-4 • 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) |

| | |
|--|---|
| | <ul style="list-style-type: none">• 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)• Wechselnde aktuelle Online-Literatur |
|--|---|

| | | | |
|---|---|-----------------------------|---------------------|
| Modulbezeichnung | 16500 Formale Grundlagen | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 16500 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Seminar Formale Grundlagen | | |
| Studiensemester | 2 | | |
| Modulverantwortliche(r) | Prof. Dr. Walter Hower | | |
| Dozent(in) | Prof. Dr. Walter Hower | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 2 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung & Seminar: | 4 SWS, Gruppengröße bis 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Seminar | 60 h | 90 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 11000 Mathematik 1 | | |
| | Die Studierenden kennen <ul style="list-style-type: none"> • Aussagen, Definitionen, Sätze • Beweis-Prinzipien • Boole'sche Algebra | | |
| Modulziele / Angestrebte Lernergebnisse | Kenntnisse Die Studierenden kennen <ul style="list-style-type: none"> • Komplexitäts-Theorie • Sprachen • Chomsky-Hierarchie • Automaten • prinzipielle Berechnungsgrenzen | | |

| | |
|--|---|
| | <p>Fertigkeiten Die Studierenden können</p> <ul style="list-style-type: none"> • gegebene Probleme analysieren • Grammatiken schreiben • Automaten erstellen <p>Kompetenzen Die Studierenden sind fähig,</p> <ul style="list-style-type: none"> • mathematik-basierte Strukturen aufzubauen • Probleme in Komplexitäts-Klassen einzuordnen • berechenbare von unberechenbaren Problemen abzugrenzen <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben |
| Inhalt | <p>Vorlesung</p> <ul style="list-style-type: none"> • Strukturelle Induktion, Ordinalzahlen, Potenzmenge, Überabzählbarkeit • Komplexität (Klassen P/(co-)NP, Reduzierbarkeit, Euler-Kreis, TSP) • Sprachen (Alphabet, Strings, Grammatiken, Chomsky-Hierarchie) • Automaten (Endlicher Automat, Keller-Automat, LBA, TM – jeweils in deterministischer und nicht-deterministischer Variante) • (Un-)Berechenbarkeit (Beispiele, Halte-Problem, Diagonalisierung) <p>Seminar</p> <ul style="list-style-type: none"> • selbstständige Erarbeitung und Darbietung ausgewählter Inhalte |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur (90 min), benotet Referat, unbenotet |
| Medienformen | Vorlesung mit Beamer, Tafel, Skript physisch sowie digital (über Lernplattform) |
| Literatur | Walter Hower: Diskrete Mathematik, Oldenbourg Wissenschaftsverlag, 2010; ISBN 978-3-486-58627-5 |

| | |
|--|--|
| | <p>Mikhail J. Atallah; Marina Blanton (eds.): Algorithms and Theory of Computation Handbook, 2nd edition – 2 Volume Set, Chapman & Hall / CRC / Taylor & Francis, 2010, ISBN 978-1-58488-818-5</p> <p>J. E. Hopcroft; R. Motwani; J. D. Ullman: Introduction to Automata Theory, Languages, and Computation, 3rd (internat.) edition, Pearson / Addison-Wesley, 2007, ISBN 978-0-321-47617-3</p> <p>H. R. Lewis, C. H. Papadimitriou: Elements of the Theory of Computation, 2nd edition, Prentice Hall / Pearson, 1998, ISBN 978-0-13-262478-7</p> <p>Arindama Singh: Elements of Computation Theory, Springer, 2009, ISBN 978-1-84882-496-6</p> |
|--|--|

| | | | |
|--------------------------------------|--|---|---------------------|
| Modulbezeichnung | 16600 Web-Anwendungen 1 | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 16600 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Web-Anwendungen 1 Praktikum Web-Anwendungen 1 | | |
| Studiensemester | 2 | | |
| Modulverantwortliche(r) | Prof. Dr. German Nemirovski | | |
| Dozent(in) | Prof. Dr. German Nemirovski | | |
| Sprache | Deutsch, bei Bedarf Englisch (muss vor Semesterbeginn geäußert werden) | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 2 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung & Übungen: | 1 SWS, Gruppengröße bis 150 | |
| | Praktikum: | 1 SWS, Gruppengröße bis 20 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 15 h | 15 h |
| | Praktikum | 15 h | 30 h |
| | Summe: 150h (2,5 * 30 Std./ECTS) | 20 h | 75 h |
| Kreditpunkte (ECTS) | 2,5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 11500 Einführung Informatik 12500 Einführung IT Security Kenntnisse Studierenden kennen <ul style="list-style-type: none"> • Netzwerke einführend • IT Sicherheit einführend | | |

| | |
|--|--|
| <p>Modulziele / Angestrebte Lernergebnisse</p> | <p>Kenntnisse</p> <p>Die Studierenden kennen</p> <ul style="list-style-type: none"> • typische Merkmale von Web-Anwendungen • die Grundlage der HTML, XHTML • Die Grundlagen von CSS • Die Grundlagen von JavaScript und JQuery <p>Fertigkeiten</p> <p>Die Studierenden sind in der Lage</p> <ul style="list-style-type: none"> • Konzeption, Design und Umsetzung einer responsiven Web-Site <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • Sind in der Lage die Anforderungen eines Kunden in Bezug auf die Struktur einer einfachen Webseite zu verstehen und umzusetzen <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • haben ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um Anwendungs- und Softwaresysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren |
| <p>Inhalt</p> | <p>Vorlesung</p> <ul style="list-style-type: none"> • Typische Merkmale von responsiven modernen Web-Seiten • HTTP-Protokoll • die Grundlage der HTML, XHTML • die Grundlagen von CSS • die Grundlagen von JavaScript • JavaScript und CSS Frameworks am beispiel von JQuery und Bootsrap |
| <p>Studien-/Prüfungsleistungen/ Prüfungsformen</p> | <p>Studienarbeit benotet.</p> |
| <p>Medienformen</p> | <p>Vorlesung mit Beamer, Skript in PDF-Format über Lernplattform; Übungen und Praktika in einem Labor (Computer-Pool)</p> |
| <p>Literatur</p> | <p>Jürgen Wolf, HTML5 und CSS3 : das umfassende Handbuch, Rheinwerk Computing; Auflage: 2, 2016, ISBN: 3836241587</p> <p>Kai Günster, Schrödinger lernt HTML5, CSS3 und JavaScript: Das etwas andere Fachbuch, Rheinwerk Computing, 2016, ISBN: 3836242575</p> |

| | |
|--|--|
| | <p>Philipp Ackermann JavaScript: Das umfassende Handbuch für Einsteiger, Fortgeschrittene und Profis, Rheinwerk Computing, 2016, ISBN: 3836238381</p> <p>https://www.w3schools.com/</p> |
|--|--|



Semester 3

| Modulbezeichnung | 21000 Sichere Datenbanken | | | | | | | | | | | | | | | | | | | | | |
|--------------------------------------|---|--------------------------|----------------|---------------------|---------------------------|------|------|---------------------|------|------|--------------------------|------|------|--------------------|------|------|-------|--|--|-------------------------------------|------|-------|
| ggf. Modulniveau | | | | | | | | | | | | | | | | | | | | | | |
| ggf. Kürzel | 21000 | | | | | | | | | | | | | | | | | | | | | |
| ggf. Untertitel | | | | | | | | | | | | | | | | | | | | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Datenbanken Grundlagen Praktikum Datenbanken Grundlagen Vorlesung & Übungen Sicherheit der Datenbanken Praktikum Datenbanken Sicherheit der Datenbanken | | | | | | | | | | | | | | | | | | | | | |
| Studiensemester | 3 | | | | | | | | | | | | | | | | | | | | | |
| Modulverantwortliche(r) | Prof. H. Morgenstern | | | | | | | | | | | | | | | | | | | | | |
| Dozent(in) | Prof. Dr. T. Heer, Prof. Dr. M. Rieger, Prof. H. Morgenstern, Prof. T. Eppler, Prof. J. Röhrle | | | | | | | | | | | | | | | | | | | | | |
| Sprache | Deutsch, bei Bedarf Englisch (muss vor Semesterbeginn geäußert werden) | | | | | | | | | | | | | | | | | | | | | |
| Zuordnung zum Curriculum | Studiengang: IT Security, Technische Informatik Wahlrichtung: - Wahl/Pflicht: Pflicht Semester: 3 Turnus: jedes Semester | | | | | | | | | | | | | | | | | | | | | |
| Lehrform / SWS | Vorlesung DB Grundlagen: 2 SWS, Gruppengröße bis 150 Praktikum DB Grundlagen: 1 SWS, Gruppengröße 20 Vorlesung Sicherheit der DB: 1 SWS, Gruppengröße bis 150 Praktikum Sicherheit der DB: 1 SWS, Gruppengröße 20 | | | | | | | | | | | | | | | | | | | | | |
| Arbeitsaufwand | <table border="0"> <thead> <tr> <th><i>Veranstaltung/Art</i></th> <th><i>Präsenz</i></th> <th><i>Eigenstudium</i></th> </tr> </thead> <tbody> <tr> <td>Vorlesung & Üb. DB Grund.</td> <td>45 h</td> <td>55 h</td> </tr> <tr> <td>Praktikum DB Grund.</td> <td>15 h</td> <td>30 h</td> </tr> <tr> <td>Vorlesung & Üb. Sich. DB</td> <td>15 h</td> <td>20 h</td> </tr> <tr> <td>Praktikum Sich. DB</td> <td>15 h</td> <td>30 h</td> </tr> <tr> <td colspan="3"><hr/></td> </tr> <tr> <td>Summe: 150h (7,5 * 30 Std./ECTS)</td> <td>90 h</td> <td>135 h</td> </tr> </tbody> </table> | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> | Vorlesung & Üb. DB Grund. | 45 h | 55 h | Praktikum DB Grund. | 15 h | 30 h | Vorlesung & Üb. Sich. DB | 15 h | 20 h | Praktikum Sich. DB | 15 h | 30 h | <hr/> | | | Summe: 150h (7,5 * 30 Std./ECTS) | 90 h | 135 h |
| <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> | | | | | | | | | | | | | | | | | | | | |
| Vorlesung & Üb. DB Grund. | 45 h | 55 h | | | | | | | | | | | | | | | | | | | | |
| Praktikum DB Grund. | 15 h | 30 h | | | | | | | | | | | | | | | | | | | | |
| Vorlesung & Üb. Sich. DB | 15 h | 20 h | | | | | | | | | | | | | | | | | | | | |
| Praktikum Sich. DB | 15 h | 30 h | | | | | | | | | | | | | | | | | | | | |
| <hr/> | | | | | | | | | | | | | | | | | | | | | | |
| Summe: 150h (7,5 * 30 Std./ECTS) | 90 h | 135 h | | | | | | | | | | | | | | | | | | | | |
| Kreditpunkte (ECTS) | 7,5 | | | | | | | | | | | | | | | | | | | | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | | | | | | | | | | | | | | | | | | | | |
| Empfohlene | 12000 Programmierung 1 | | | | | | | | | | | | | | | | | | | | | |

| | |
|-------------------------------|--|
| Voraussetzungen | 12500 Einführung IT Security 14500 Programmierung 2 15000 Betriebssysteme |
| Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden kennen</p> <ul style="list-style-type: none"> • 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) <p>Fertigkeiten</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> • 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 Sicherheits Gesichtspunkten bewerten (Auditing) <p>Kompetenzen</p> <p>Die Studierenden sind fähig</p> <ul style="list-style-type: none"> • gegebene Aufgabenstellungen aus dem Bereich der Wirtschaftsinformatik, der Technischen Informatik und der IT-Security zu analysieren und als Datenmodell für den Einsatz von Datenbankanwendungen zu realisieren |

| | |
|---------------|--|
| | <ul style="list-style-type: none"> • komplexe Anwendungssituationen zu erfassen und Daten vermittlems SQL effektiv aufzubereiten und ggf. zu visualisieren • ein konkretes Datenbanksystem professionell einzusetzen • Sicherheitsrisiken in der Konfiguration und der Struktur eines Datenbanksystems zu erkennen und zu behandeln <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind in der Lage, übergreifende Prozesse zwischen Wirtschaftseinheiten (Unternehmen, Verwaltungseinheiten) durch Anwendungssoftware zu unterstützen • haben ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um betriebliche Anwendungssysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren • können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben • sind in der Lage Systeme sowie Anwendungen zu analysieren, entwerfen, entwickeln und pflegen, sodass sie den heutigen Maßstäben an die Sicherheit gerecht werden • 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 |
| <p>Inhalt</p> | <p>Vorlesung, Übungen und Praktikum</p> <ul style="list-style-type: none"> • der konzeptionelle Datenbankentwurf • Referenzmodelle • Begriffsbildung und Abstraktionskonzepte, Semantische Datenmodelle • das Entity-Relationship-Modell • das Objekttypenmodell • das Generische Semantische Datenmodell • Grenzen des ER-basierten Datenbank-Entwurfs • Normalformenlehre • Integritätsbedingungen als Maß für die Qualität der Daten und Transaktionen • die Datenbanksprache SQL • Nachteile des (flachen) Relationenmodells |

| | |
|--|--|
| | <ul style="list-style-type: none"> • Objektorientierung in Datenbanksystemen • Objektrelationale DBMS • Schema- und Sichtdefinition • Einführung in die Spracheinbettung von SQL in Programmiersprachen (z.B. in Java vermittelt JDBC - Java Database Connectivity) • Transaktionen aus Implementierungssicht • Anwendungssituationen von Transaktionen unter verschiedenen Isolationsmodi • Methoden zur Implementierung von Datensicherungs- und Recovery-Maßnahmen • Modellierung von Zugriffsbeschränkungen, Rechtemodellen, Sicherungen, Benutzerrechten, Rollen, Protokolldateien • Grundlagen des Datenschutzes und Umgang mit sicherheitskritischen Informationen • Speicherung von Passwörtern und vertraulichen Daten • Verschlüsselte Datenbanken und Schutz von Datenbanksystemen • Auditing von Datenbanken |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur 120 min, benotet Praktische Arbeit, unbenotet |
| Medienformen | Skript in PDF-Format; Implementierung konkreter Anwendungsfälle und Visualisierung mit Beamer; Übungen und Tests in einem Labor. (Materialien sind z.T. in Englisch) |
| Literatur | <p>Wieken, J.-H.: SQL - Einstieg für Fortgeschrittene, Addison Wesley, 2008</p> <p>Matthiessen, G.; Unterstein, M.: Relationale Datenbanken und Standard-SQL, Addison Wesley, 2007</p> <p>Oracle 11g Release 2 für den DBA, Addison Wesley, 2013</p> <p>Elmasri R., S. Navathe: Fundamentals of Database Systems, 6th ed., Addison Wesley, 2011</p> <p>Kroenke, D.M.; Auer, D.: Database Processing, Prentice Hall, 2010</p> <p>Kroenke, D.M.; Auer, D.: Database Concepts, 5th ed., Prentice Hall, 2011</p> <p>Harrison, G.: Oracle Performance Survival Guide: A Systematic Approach to Database Optimization, Prentice Hall, 2010</p> <p>Connolly, T.M.; Begg, C.: Database Systems: A Practical Approach to Design, Implementation and Management, 5th ed., Prentice Hall, 2010</p> <p>Garcia-Molina, H.; Ullman, J.D., Widom, J.: Database Systems. The Complete Book, Prentice Hall, 2009</p> <p>van der Lans, R.F.: Introduction to SQL: Mastering the Relational Database Language, 5th ed., Addison Wesley, 2013</p> <p>Greenwald, R.; Stackowiak, R.; Stern, J.: Oracle Essentials, O'Reilly, 2012</p> |

| | |
|--|--|
| | <p>Feuerstein, S.: Oracle PL/SQL - Best Practices, O' Reilly, 2007</p> <p>Feuerstein, S. , Pribyl, B.: Oracle PL/SQL Programming, O' Reilly, 2007</p> <p>Elliot, J., O'Brian, T.M., Fowler, R.: Harnessing Hibernate, O' Reilly, 2008</p> <p>Wehr, H., Müller, B.: Java Persistence API mit Hibernate, Addison Wesley, 2007</p> <p>Bauer, Chr.; King, G.: Hibernate in Action. Manning Pub., 2004</p> <p>Elliot, J., O'Brian, T.M., Fowler, R.: Harnessing Hibernate, O' Reilly, 2008</p> <p>Wehr, H., Müller, B.: Java Persistence API mit Hibernate, Addison Wesley, 2012</p> <p>Bauer, Chr.; King, G.: Hibernate in Action. Manning Pub., 2012</p> <p>Date, C.J.; An Introduction to Database Systems, Addison-Wesley, 2003</p> <p>Natan, R.B.; Smplementing Database Security and Auditing, Elsevier, 2005</p> |
|--|--|

| | | | |
|--------------------------------------|---|---|--------------|
| Modulbezeichnung | 15500 Algorithmik | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 15500 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Algorithmik | | |
| Studiensemester | 2 | | |
| Modulverantwortliche(r) | Prof. Dr. Tobias Häberlein, Prof. Dr. Walter Hower | | |
| Dozent(in) | Prof. Dr. Tobias Häberlein, Prof. Dr. Walter Hower | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 2 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung & Übungen: | 2 SWS, Gruppengröße bis 150 | |
| Arbeitsaufwand | Veranstaltung/Art | Präsenz | Eigenstudium |
| | Vorlesung, Übungen | 30h | 45h |
| | Summe: 75h (2,5 * 30 Std./ECTS) | 30h | 45h |
| Kreditpunkte (ECTS) | 2,5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 11000 Mathematik 1 Die Studierenden <ul style="list-style-type: none"> • kennen die Bedeutung der grundlegenden mathematischen und logischen Begriffe wie Mengen, Funktionen, Relationen, Aussagen, Definitionen, Sätze, Beweise • kennen die grundlegenden Begriffe, Strukturen und Sätze der Analysis, wie z.B. Körper, Funktionsklassen, Grenzwerte von Folgen und Reihen, Stetigkeit, Ableitung, Satz von Taylor, Integrale, Trigonometrie • kennen die grundlegenden Begriffe und Sätze der Linearen Algebra und Analytischen Geometrie wie z.B. Vektor, Gerade, Ebene, Vektorraum, Lineares Gleichungssystem, lineare Abbildung, Matrix, Determinante, Projektion | | |

| | |
|--|--|
| <p>Modulziele / Angestrebte Lernergebnisse</p> | <p>Kenntnisse</p> <p>Die Studierenden kennen</p> <ul style="list-style-type: none"> • die Grundlagen der Komplexitätstheorie • die Methoden des Entwurfs und der Analyse von Algorithmen • wichtige grundlegende Algorithmen <p>Fertigkeiten</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind in der Lage, Standard-Berechnungsverfahren anzuwenden • die Größenordnung der Laufzeit von Algorithmen abzuschätzen <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind in der Lage, Problemlösungs-Strategien auf Informatik-Probleme anzuwenden • 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 <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise beschreiben |
| <p>Inhalt</p> | <p>Vorlesung</p> <ul style="list-style-type: none"> • Kostenmaße und deren Notation • Hashing • Suchen und Sortieren • Rekurrenz-Relation • Problemlösungs-Strategien • Anwendung von Programmier-Schnittstellen zu Algorithmen |
| <p>Studien-/Prüfungsleistungen/ Prüfungsformen</p> | <p>Klausur 60, benotet</p> |
| <p>Medienformen</p> | <p>Beamer, Tafel</p> |

| | |
|-----------|---|
| Literatur | <p>Walter Hower: <i>Diskrete Mathematik</i>, Oldenbourg Wissenschaftsverlag, 2010, ISBN 978-3-486-58627-5</p> <p>Anany Levitin: <i>Introduction to The Design and Analysis of Algorithms</i>, 3rd (internat.) edition, Pearson Higher Education, 2012, ISBN 978-0-273-76411-3</p> <p>T. H. Cormen, C. E. Leiserson, R. L. Rivest, C. Stein: <i>Introduction to Algorithms</i>, 3rd (internat.) edition, MIT Press, 2009, ISBN 978-0-262-53305-8</p> <p>Kurt Mehlhorn: <i>Effiziente Algorithmen</i>, Teubner, 1977, ISBN 9783519023432</p> <p>Kurt Mehlhorn, Peter Sanders: <i>Algorithmen und Datenstrukturen</i>, eXamen.press/Springer, 2011, ISBN 978-3-642-05471-6</p> <p>R. Sedgewick: <i>Algorithmen in Java</i>, 3. Auflage, Pearson Studium, München, ISBN 2003; 978-3-8273-7072-3</p> |
|-----------|---|

| | | | |
|---|--|------------------------------------|---------------------|
| Modulbezeichnung | 21100 Betriebswirtschaftslehre und Management | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 21100 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Betriebswirtschaftslehre und Management | | |
| Studiensemester | 3 | | |
| Modulverantwortliche(r) | Prof. Dr. Philipp Lindenmayer | | |
| Dozent(in) | Prof. Dr. Philipp Lindenmayer | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT Security, Wirtschaftsinformatik | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 3 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung & Übungen: | 2 SWS, Gruppengröße bis 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 30 h | 45 h |
| | Summe: 75h (2,5 * 30 Std./ECTS) | 30 h | 45 h |
| Kreditpunkte (ECTS) | 2,5 | | |
| Voraussetzungen nach Prüfungsordnung | keine | | |
| Empfohlene Voraussetzungen | keine | | |
| Modulziele / Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • verstehen grundlegende betriebswirtschaftliche Zusammenhänge, gesetzte Ziele sowie die wesentlichen Schritte zur Umsetzung und Verfolgung dieser Ziele. • erlangen ein grundlegendes Verständnis zu Aufgaben und wirtschaftlichen Fragestellungen der jeweiligen betrieblichen Funktionen in Unternehmen. • verstehen die Bedeutung der Kundenorientierung des gesamten unternehmerischen Handelns und lernen das Unternehmen als Modell einer Ablauf- und Aufbauorganisation kennen. | | |

| | |
|--------|---|
| | <p>Fertigkeiten</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • 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. <p>Kompetenzen</p> <ul style="list-style-type: none"> • haben praxisorientierte Kenntnisse der Wirtschaftswissenschaften und ein Grundverständnis für betriebliche Problemstellungen und der Methoden ihrer Beschreibung / Spezifikation und Beurteilung • haben einen Überblick der Gesamtheit geschäftlicher Abläufe in mittelständischen Unternehmen (KMU) bis hin zum gehobenen Mittelstand („Hidden Champions“) <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • 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 • sind sich ihrer Verantwortung gegenüber Individuen und der Gesellschaft beim Umgang mit Sicherheitsrelevanten Informationen und Sicherheitsmethoden bewusst • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams |
| Inhalt | <p>Vorlesung</p> <ul style="list-style-type: none"> • Herkunft und wissenschaftlicher Ansatz der Betriebswirtschaftslehre • Grundlagen betriebswirtschaftlicher Theorien • Rechtsformen und Unternehmensverfassung • Betriebliche Zielbildung und –systeme • Das Unternehmen als ablauf- und aufbauorganisatorisches Konstrukt • Betriebliche Strukturen und darin eingebettete Funktionen • Kern-, Hilfs-, und Entscheidungsprozesse der betrieblichen Güter- und Dienstleistungserstellung |

| | |
|--|--|
| | <ul style="list-style-type: none"> Zusammenhänge und Wirkungen betriebswirtschaftlicher Entscheidungen auf den Unternehmenserfolg <p>Übungen / Fallstudie(n)</p> <ul style="list-style-type: none"> zu ausgewählten Themen aus der Vorlesung, teils in Gruppenarbeit |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur 60 min., benotet |
| Medienformen | Vorlesung mit Beamer, Tafel, Skript physisch |
| Literatur | <p>Schmalen, H.; Pechtl, H., Grundlagen und Probleme der Betriebswirtschaft, 15. Auflage, Schäffer Poeschel, 2013</p> <p>Bernecker, M.: Grundlagen der Betriebswirtschaftslehre: BWL, 4. Auflage, Johanna Verlag, 2011</p> <p>Hopfenbeck, W.: Allgemeine Betriebswirtschafts- und Managementlehre, o. A., o. V., 2002</p> <p>Jung, H.: Allgemeine BWL, 12. Auflage, Oldenbourg Verlag, 2010</p> <p>Schierenbeck, H.; Wöhle, C.: Grundzüge der Betriebswirtschaftslehre, 17. Auflage, Oldenbourg Verlag, 2008</p> <p>Thommen, J.-P.; Achleitner, A.-K.: Allgemeine BWL - Umfassende Einführung aus management-orientierter Sicht, 7. Auflage, Gabler Verlag, 2012</p> <p>Wöhe, G.: Einführung in die allgemeine BWL, 25. Auflage, Vahlen Verlag, 2013</p> |

| | | | |
|--------------------------------------|--|------------------------------------|---------------------|
| Modulbezeichnung | 21200 Netzwerke | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 21200 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Netzwerke Praktikum Netzwerke | | |
| Studiensemester | 3 | | |
| Modulverantwortliche(r) | Prof. Dr. Tobias Heer | | |
| Dozent(in) | Prof. Dr. Tobias Heer | | |
| Sprache | Deutsch, (deutsches und englisches Literaturstudium erforderlich) | | |
| Zuordnung zum Curriculum | Studiengang: | Technische Informatik, IT-Security | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflicht | |
| | Semester: | 3 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung: 3 SWS, Gruppengröße bis 150 Praktikum: 1 SWS, Gruppengröße 20 | | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 45 h | 45 h |
| | Praktikum | 15 h | 45 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 11500 Einführung Informatik 12500 Einführung IT Security 15000 Betriebssysteme Kenntnisse in C-Programmierung | | |
| Angestrebte Lernergebnisse | Kenntnisse Die Studierenden | | |

| | |
|--|--|
| | <ul style="list-style-type: none"> • kennen das ISO/OSI-Modell und das TCP/IP Modell • kennen die grundlegenden Geräte im Internet wie Switches und Router • kennen die Funktionen und die Funktionsweise der gängigen Protokolle des TCP/IP Kommunikations-Stacks • kennen den Aufbau von IP- und MAC-Adressen sowie DNS Namen und deren Adressraum • Kennen die Funktion von CSMA/CD und CSMA/CA Netzwerken (Ethernet und WLAN) • Kennen die Möglichkeiten zur physischen Übertragung von Daten • Verstehen den Aufbau und die innere Funktion von E-Mail-Systemen und HTTP/1.1.1/2 <p>Fertigkeiten</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> • Netzwerke aufbauen und analysieren • Router und Switches konfigurieren • Netzwerkverkehr analysieren • Limitierungen von Netzwerktechnologien einschätzen • Netzwerkanwendungen entwickeln <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind fähig die Begriffe im Bereich Netze zu verstehen und aktiv anzuwenden • sind in der Lage Netzwerke zu entwerfen, zu implementieren und zu erweitern • sind in der Lage Fehler in Netzwerken zu verstehen und zu beseitigen • sind fähig die Entwurfsentscheidungen in Netzwerkprotokollen zu durchdringen und eigene Protokolle zu entwerfen • sind in der Lage Netzwerk-Software mit der Socket Schnittstelle selbst zu entwerfen und umzusetzen <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind dazu befähigt, Daten und Prozessmodelle mit gängigen Modellierungsmethoden zu entwerfen, zu analysieren und Heuristiken für die Optimierung anzuwenden • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • verfügen über die zur Erfüllung von Anforderungen der Berufspraxis notwendigen persönlichen Kompetenzen: eigen-verantwortliches Handeln, Zeitmanagement, Selbstorganisation |
|--|--|

| | |
|--------|--|
| | <ul style="list-style-type: none"> • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben • sind in der Lage Systeme sowie Anwendungen zu analysieren, entwerfen, entwickeln und pflegen, sodass sie den heutigen Maßstäben an die Sicherheit gerecht werden • 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 • 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 • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams |
| Inhalt | <p>Grundlagen der Netzwerkkommunikation</p> <ul style="list-style-type: none"> • Kommunikationsmodelle • Netzwerktopologien und Schichtenmodelle (ISO/OSI und TCP/IP) • Aufbau von Kommunikationsprotokollen und vernetzten Systemen <p>Kommunikationsprotokolle des TCP/IP Protokoll-Stacks</p> <ul style="list-style-type: none"> • 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 <p>Netzwerkpraxis und Socket Programmierung</p> <ul style="list-style-type: none"> • 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 |

| | |
|--|--|
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur 90 min, benotet Praktische Arbeit, unbenotet |
| Medienformen | Skript in PDF-Format; Implementierung konkreter Anwendungsfälle und Visualisierung mit Beamer; Übungen und Tests in einem Labor. (Materialien sind z.T. in Englisch) |
| Literatur | Kurose J. und Ross K.: Computernetzwerke : der Top-Down-Ansatz Pearson Verlag, 2008 Andrew S. Tanenbaum: Computernetzwerke, Pearson-Verlag, 3. Auflage, 2000 |

| | | | |
|--------------------------------------|---|----------------|---------------------|
| Modulbezeichnung | 21300 Rechnertechnik | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 21300 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Rechnertechnik Praktikum Rechnertechnik | | |
| Studiensemester | 3 | | |
| Modulverantwortliche(r) | Prof. Dr. Joachim Gerlach | | |
| Dozent(in) | Prof. Dr. Joachim Gerlach | | |
| Sprache | Deutsch, (deutsches und englisches Literaturstudium erforderlich) | | |
| Zuordnung zum Curriculum | Studiengang: | IT Security | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflicht | |
| | Semester: | 3 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung: 4 SWS, Gruppengröße bis 150 | | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 30 h | 45 h |
| | Praktikum | 30 h | 45 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | keine | | |
| Empfohlene Voraussetzungen | Programmierung 2 (Grundlagen der Programmierung, Programmentwicklung in C) | | |
| Angestrebte Lernergebnisse | <p>Vermittlung von Kenntnissen bzgl. des Aufbaus, der Programmierung und der Anwendung von Mikrorechnersystemen. Einführung in die Programmierung von Mikroprozessoren in Assembler und in C. Kenntnis der Architektur und Funktionsweise von Mikroprozessoren und Mikrorechnersystemen.</p> <p>Sicherheit von Mikrorechnersystemen, Schwachstellen und Angriffsszenarien auf Hardware-naher Ebene.</p> | | |

| | |
|--|---|
| | <p>Kenntnisse</p> <p>Die Studierenden kennen</p> <ul style="list-style-type: none"> • kennen den Aufbau, der Programmierung und die Anwendung von Mikrorechnersystemen • die Architektur und Funktionsweise von Mikroprozessoren und Mikrorechnersystemen <p>Fertigkeiten</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> • Mikroprozessoren in Assembler und in C programmieren <p>Kompetenzen</p> <p>Die Studierenden sind in der Lage</p> <ul style="list-style-type: none"> • das Zusammenspiel von Hardware und Software innerhalb von Mikrorechnersystemen zu verstehen und für den Aufbau von eingebetteten Hardware/Software-Systemlösungen einzusetzen • die Sicherheit von Mikrorechnersystemen, Schwachstellen und Angriffsszenarien auf Hardware-naher Ebene zu verstehen und zu beurteilen <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen • 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 • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams • sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt • sind in der Lage Systeme sowie Anwendungen zu analysieren, entwerfen, entwickeln und pflegen, sodass sie den heutigen Maßstäben an die Sicherheit gerecht werden |
|--|---|

| | |
|--|--|
| Inhalt | <p>Vorlesung</p> <ul style="list-style-type: none"> • Geschichtliche Entwicklung der Mikroprozessortechnik • Architektur und Funktionsweise von Mikroprozessoren <p>Programmierung von Mikroprozessorsystemen</p> <ul style="list-style-type: none"> • Grundlagen der Assemblerprogrammieren • Unterprogrammtechniken • Synchronisation & Interrupt-Handling • Hardware-nahe Programmierung in Assembler und C <p>Praktikum</p> <ul style="list-style-type: none"> • Programmieren eines Mikroprozessors in Assembler auf Basis eines Befehlssatzemulators • Programmieren eines Mikroprozessors in Assembler und Hardware-nahem C auf Basis eines Einplatinencomputers |
| Studien- /Prüfungsleistungen/ Prüfungsformen | Klausur 90 Min, Benotet Laborarbeit unbenotet |
| Medienformen | Vorlesung: PC mit Beamer, Folienskript Praktikum: Arbeiten am Rechner und an Mikrocontroller-Boards im Labor |
| Literatur | <p>Patterson D.A., Hennessy J.L.: Computer Organization and Design. Morgan Kaufmann</p> <p>Bode A., Karl W., Ungerer T.: Rechnerorganisation und -entwurf. Spektrum Akademischer Verlag</p> <p>Wüst K.: Mikroprozessortechnik. Vieweg+Teubner Verlag.</p> <p>Beierlein T., Hagenbruch O.: Taschenbuch Mikroprozessortechnik. Carl Hanser Verlag</p> |

| Modulbezeichnung | 21400 Kryptologie 2 | | | | | | | | | | | | |
|--------------------------------------|---|--------------------------|----------------|---------------------|---------------------|------|------|-----------|--------|--------|-------------------------------------|--------|---------|
| ggf. Modulniveau | | | | | | | | | | | | | |
| ggf. Kürzel | 21400 | | | | | | | | | | | | |
| ggf. Untertitel | | | | | | | | | | | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Kryptologie 2 Praktikum Kryptologie 2 | | | | | | | | | | | | |
| Studiensemester | 3 | | | | | | | | | | | | |
| Modulverantwortliche(r) | Prof. Dr. Tobias Häberlein | | | | | | | | | | | | |
| Dozent(in) | Prof. Dr. Tobias Häberlein | | | | | | | | | | | | |
| Sprache | Deutsch, (deutsches und englisches Literaturstudium erforderlich) | | | | | | | | | | | | |
| Zuordnung zum Curriculum | Studiengang: IT Security Wahlrichtung: - Wahl/Pflicht: Pflicht Semester: 3 Turnus: jedes Semester | | | | | | | | | | | | |
| Lehrform / SWS | Vorlesung: 4 SWS, Gruppengröße bis 150 Praktikum: 2 SWS, Gruppengröße 20 | | | | | | | | | | | | |
| Arbeitsaufwand | <table border="1"> <thead> <tr> <th><i>Veranstaltung/Art</i></th> <th><i>Präsenz</i></th> <th><i>Eigenstudium</i></th> </tr> </thead> <tbody> <tr> <td>Vorlesung & Übungen</td> <td>45 h</td> <td>75 h</td> </tr> <tr> <td>Praktikum</td> <td>22,5 h</td> <td>82,5 h</td> </tr> <tr> <td>Summe: 225h (7,5 * 30 Std./ECTS)</td> <td>67,5 h</td> <td>157,5 h</td> </tr> </tbody> </table> | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> | Vorlesung & Übungen | 45 h | 75 h | Praktikum | 22,5 h | 82,5 h | Summe: 225h (7,5 * 30 Std./ECTS) | 67,5 h | 157,5 h |
| <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> | | | | | | | | | | | |
| Vorlesung & Übungen | 45 h | 75 h | | | | | | | | | | | |
| Praktikum | 22,5 h | 82,5 h | | | | | | | | | | | |
| Summe: 225h (7,5 * 30 Std./ECTS) | 67,5 h | 157,5 h | | | | | | | | | | | |
| Kreditpunkte (ECTS) | 7,5 | | | | | | | | | | | | |
| Voraussetzungen nach Prüfungsordnung | Kryptologie 1 | | | | | | | | | | | | |
| Empfohlene Voraussetzungen | keine | | | | | | | | | | | | |
| Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden kennen die vorgestellten kryptologischen Konzepte und Verfahren.</p> <p>Fertigkeiten</p> | | | | | | | | | | | | |

| | |
|--------|--|
| | <p>Die Studierenden können imperative, objektorientierte und funktionale Aspekte der Programmiersprache Python zur Lösung von Problemstellungen selbstständig einsetzen und können daraus selbstständig lauffähige wohlstrukturierte Programme entwickeln.</p> <p>Kompetenzen</p> <ul style="list-style-type: none"> • Die Studierenden sind in der Lage die betrachteten Verfahren anzuwenden, gegeneinander abzuwägen, einfache Sicherheitsbetrachtungen anzustellen. 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. • 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. • Die Studierenden sind in der Lage, Machbarkeit, Sicherheit und Innovationsgrad angestrebter Sicherheitslösungen aus kryptologisch-mathematischer Sicht einschätzen <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei</p> <ul style="list-style-type: none"> • WIN-2: Absolventen des Studiengangs sind dazu befähigt, Daten und Prozessmodelle mit gängigen Modellierungsmethoden zu entwerfen, zu analysieren und Heuristiken für die Optimierung anzuwenden. • WIN-4: Absolventen des Studiengangs sind in der Lage, übergreifende Prozesse zwischen Wirtschaftseinheiten (Unternehmen, Verwaltungseinheiten) durch Anwendungs-Software zu unterstützen. • INF-2: Absolventen des Studiengangs können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen. • ITS-1: Absolventen des Studiengangs sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt. • ITS-3: Absolventen des Studiengangs 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 |
| Inhalt | <ul style="list-style-type: none"> • Klassische Verfahrenen der Kryptographie • Symmetrische Verfahren (DES, AES) • Differentielle und Lineare Attacken • Seitenkanalattacken • Endliche Körper und $GF(pq)$ • Betriebsmodi |

| | |
|--|--|
| | <ul style="list-style-type: none"> • 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 |
| <p>Studien-/Prüfungsleistungen/ Prüfungsformen</p> | <p>Klausur 120 min, benotet Laborarbeit, unbenotet</p> |
| <p>Medienformen</p> | <p>Vorlesung mit Beamer; Implementierung konkreter Anwendungsfälle und Visualisierung mit Beamer; Übungen und Tests in einem Labor</p> |
| <p>Literatur</p> | <p>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.</p> |



Semester 4

| | | | |
|--------------------------------------|---|---|---------------------|
| Modulbezeichnung | 22000 Web-Anwendungen 2 | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 22000 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Web-Anwendungen 2 Praktikum Web-Anwendungen | | |
| Studiensemester | 4 | | |
| Modulverantwortliche(r) | Prof. Dr. German Nemirovski | | |
| Dozent(in) | Prof. Dr. German Nemirovski | | |
| Sprache | Deutsch, bei Bedarf Englisch (muss vor Semesterbeginn geäußert werden) | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 4 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung & Übungen: | 3 SWS, Gruppengröße bis 150 | |
| | Praktikum: | 1 SWS, Gruppengröße bis 20 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 45 h | 15 h |
| | Praktikum | 15 h | 75 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 21200 Netzwerke 21000 Datenbanken 1 14500 Programmierung 2 12500 Einführung IT Security Kenntnisse Studierenden kennen <ul style="list-style-type: none"> die wichtigsten Netzwerk-Protokolle, wie z.B. TCP, IP, ARP, HTTP | | |

| | |
|--|--|
| | <ul style="list-style-type: none"> • das ISO-OSI Modell • die TCP-Dienste, u.a. HTTP-Dienst <p>Fertigkeiten</p> <p>Studierenden sind in der Lage,</p> <ul style="list-style-type: none"> • Daten Modelle mit Hilfe von UML und ER-Diagrammen zu entwickeln • Anwendungen mit der Programmiersprache Java zu entwickeln |
| <p>Modulziele / Angestrebte Lernergebnisse</p> | <p>Kenntnisse</p> <p>Die Studierenden kennen</p> <ul style="list-style-type: none"> • typische Merkmale von Web-Basierten Anwendungen • die Basistechnologien, wie Servlets • den unterschied zwischen Client- Server-Seitigen Steuerung • das Model-View-Controller-Modell und mindestens ein darauf basierende Framework, z.B. Java Server Faces • den Funktionsprinzip von Web Services • gängige Schwachstellen in Web Anwendungen und wie diese ausgenutzt werden können. • die Schutzmaßnahmen zu den genannten Schwachstellen • das Servlets Authentication Verfahren <p>Fertigkeiten</p> <p>Die Studierenden sind in der Lage</p> <ul style="list-style-type: none"> • Konzeption und Design einer Web-Anwendung durchzuführen • Web-Anwendungen mithilfe der JEE-Technologie zu Entwickeln • Web-Projekte mit Hilfe von Standard-IDE, wie eclipse oder Netbeans zu verwalten • Web Anwendungen methodisch auf Schwachstellen zu überprüfen, diese zu priorisieren und die Gegenmaßnahmen umzusetzen <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind in der Lage eigenständig oder im Team Web-Basierte-Anwendungen, wie die E-Commerce, Soziale Netzwerke oder Informationssysteme konzipieren und entwickeln • sind in der Lage Research , Analyse und zielgerichtete Präsentation in Bezug auf die Suche nach neuen Technologien auszuführen • sind in der Lage Web Anwendungen zielgerichtet ihrer Sicherheit betreffend zu untersuchen und zu bewerten |

| | |
|---------------|--|
| | <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind dazu befähigt, betriebliche Informations- und Anwendungssysteme samt ihrer Komponenten zu analysieren und zu entwerfen. Einen besonderen Schwerpunkt stellen dabei ERP Systeme im betrieblichen Kontext dar • haben ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um betriebliche Anwendungssysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in Bezug auf einen bestimmten Anwendungsbedarf zu verfolgen • verfügen über die zur Erfüllung von Anforderungen der Berufspraxis notwendigen persönlichen Kompetenzen: eigen-verantwortliches Handeln, Zeitmanagement, Selbstorganisation • sind in der Lage Systeme sowie Anwendungen zu analysieren, entwerfen, entwickeln und pflegen, sodass sie den heutigen Maßstäben an die Sicherheit gerecht werden • 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 • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams |
| <p>Inhalt</p> | <p>Vorlesung</p> <ul style="list-style-type: none"> • Typische Merkmale von Web-Basierten Anwendungen • HTTP-Protokoll • Grundlagen von Servlets • XML und JSON in Vergleich • JavaScript und die Client-Seitige Frameworks wie JQuery • Web Services • Web Sockets • MVC und die Serverseitige Frameworks Frameworks • Konfiguration und Deployment von Web-basierten Anwendung • Schwachstellen und die Prüfmethodik der Web-Anwendungen • Authentifizierung und Session Management aus der Perspektive der Sicherheit |

| | |
|--|---|
| | <ul style="list-style-type: none"> • Bewertung und die Priorisierung von Schwachstellen. <p>Praktikum</p> <ul style="list-style-type: none"> • Entwicklung von Web-basierten Anwendung mithilfe der JEE-Technologie • Überprüfung des Anwendung auf die Schwachstellen |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur 90 min., beide Leistungen werden gemeinsam benotet. Laborarbeit, unbenotet |
| Medienformen | Vorlesung mit Beamer, Skript in PDF-Format über Lernplattform; Übungen und Tests in einem Labor |
| Literatur | <p>Philipp Ackermann JavaScript: Das umfassende Handbuch für Einsteiger, Fortgeschrittene und Profis, Rheinwerk Computing, 2016, ISBN: 3836238381</p> <p>Alexander Salvanos, Professionell entwickeln mit Java EE 7: Das umfassende Handbuch, Galileo Computing, 2014, ISBN: 3836220040</p> <p>Beyer, Jörg; Weimer (Lahn); Schulten, Lars: Servlets & JSP von Kopf bis Fuß, O'Reilly, Köln, 2009</p> <p>Stuttard, Dafydd, and Marcus Pinto. The web application hacker's handbook: finding and exploiting security flaws. John Wiley & Sons, 2011.</p> <p>Shostack, Adam. Threat modeling: Designing for security. John Wiley & Sons, 2014.</p> <p>https://tomcat.apache.org/</p> <p>https://www.w3schools.com/</p> |

| | | | |
|---|---|-----------------------------|---------------------|
| Modulbezeichnung | 22100 Wirtschafts- und Internetrecht | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 22100 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Wirtschafts- und internetrecht Vorlesung & Übungen Datenschutz und Urheberrecht | | |
| Studiensemester | 4 | | |
| Modulverantwortliche(r) | Prof. Dr. German Nemirovski | | |
| Dozent(in) | Egorova, O. | | |
| Sprache | Deutsch, bei Bedarf Englisch (muss vor Semesterbeginn geäußert werden) | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 4 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung: | 4 SWS, Gruppengröße bis 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Wirtschafts- und internetrecht | 30 h | 45 h |
| | Datenschutz und Urheberrecht | 30 h | 45 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | Keine | | |
| Modulziele / Angestrebte Lernergebnisse | Kenntnisse Die Studierenden <ul style="list-style-type: none"> • kennen das System des deutschen Verfassungsrechts mit seinen staatstheoretischen, europarechtlichen und völkerrechtlichen Grundlagen, • haben die Rechtsnatur und die wesentlichen Eigenschaften des Völkerrechts und des Europarechts – auch im Vergleich zum nationalen Recht – verstanden. • kennen Stellung und Einordnung des sogenannten Internetrechts in das Gesamtrechtssystem und sein Verhältnis zum Medienrecht • kennen internetrechtsspezifische Problemfelder beim Einsatz des Internets als betriebliches Präsentations-, Marketing- und Vertriebsinstrument | | |

| | |
|--------|--|
| | <p>Fertigkeiten Die Studierenden</p> <ul style="list-style-type: none"> • sind in der Lage wichtige rechtliche Sachverhalte relevante zur Erstellung und zum Betrieb 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 und Datenschutz • haben einen Überblick der Gesamtheit geschäftlicher Abläufe in mittelständischen Unternehmen (KMU) bis hin zum gehobenen Mittelstand („Hidden Champions“) <p>Kompetenzen Die Studierenden</p> <ul style="list-style-type: none"> • sind sich ihrer Verantwortung gegenüber Individuen und der Gesellschaft beim Umgang mit Sicherheitsrelevanten Informationen und Sicherheitsmethoden bewusst • sind in der Lage die Zusammenhänge und die Anwendbarkeit der für das Internet relevanten Vorschriften und Gesetze sowie rechtliche Gefahren- und Fehlerquellen zu beurteilen und Ihren Arbeitseinsatz darauf hin zu richten <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei: Die Studierenden</p> <ul style="list-style-type: none"> • sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in Bezug auf einen bestimmten Anwendungsbedarf zu verfolgen |
| Inhalt | <p>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:</p> <ul style="list-style-type: none"> • 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 |

| | |
|--|---|
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur 90 min., |
| Medienformen | Vorlesung mit Beamer, Skript in PDF-Format über Lernplattform; |
| Literatur | <p>Schiffer/von Schubert (Hrsg.), Recht, Wirtschaft und Steuern im E-Business, Herne/Berlin (NWB-Verlag)</p> <p>Moritz/Dreier (Hrsg.), Rechts-Handbuch zum E-Commerce, Köln (Dr. Otto Schmidt Verlag)</p> <p>Kröger/Gimmy, Handbuch zum Internet-Recht, 2. Aufl., Berlin, Heidelberg (Springer Verlag)</p> <p>Carey/Sanders, Media Law, 3. Aufl., London (Sweet & Maxwell);</p> <p>Ladeur, Das Werberecht der elektronischen Medien, Heidelberg (Verlag Recht und Wirtschaft)</p> <p>Reed, Internet Law: Text and Materials, 2. Aufl., Cambridge (England) (Cambridge University Press)</p> <p>Verbiest, Commerce électronique: le nouveau cadre juridique, Louvains La Neuve (Belgien) (Editions Larcier)</p> <p>Spindler/Wiebe (Hrsg.), Internet Auktionen und Elektronische Marktplätze, 2. Aufl, Köln (Verlag Dr. Otto Schmidt)</p> <p>Berman, Cyberlaw, Aldershot (England) (Ashgate)</p> <p>Carr, Globalization and E-Commerce, Aldershot (England) (Ashgate)</p> <p>Aktuelle Gesetzestexte (insbesondere GG, BGB, TelemediaR, EuR, z.B. in Ausgaben des Deutschen Taschenbuch Verlages (dtv)</p> |

| | | | |
|---|---|------------------------------------|---------------------|
| Modulbezeichnung | 22200 Betriebssicherheit | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 22200 | | |
| ggf. Untertitel | | | |
| Lehrveranstaltung | Vorlesung und Übungen Betriebssicherheit Praktikum Betriebssicherheit | | |
| Studiensemester | 4 | | |
| Modulverantwortliche(r) | Prof. Dr. Derk Rembold | | |
| Dozent(in) | Prof. Dr. Derk Rembold | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 4 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung & Übungen: | 3 SWS, Gruppengröße bis 150 | |
| | Praktikum: | 1 SWS, Gruppengröße bis 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung, Übungen | 45 h | 40 h |
| | Praktikum | 15 h | 50 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 21300 Rechnertechnik 11000 Mathematik 1 14000 Mathematik 2 | | |
| Modulziele / Angestrebte Lernergebnisse | Kenntnisse Die Studierenden <ul style="list-style-type: none"> • sicherheitsbezogene Normen und Standards • Analysemethoden, um System mit sicherheitstechnische Problemen bezüglich des Risikos zu quantifizieren • Sicherheitstechnisch relevante Modelle für technische Systeme | | |

| | |
|--|--|
| | <p>Fertigkeiten</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • technische Systeme unter Berücksichtigung des Risikoverhaltens zu modellieren • technische Systeme auf Zuverlässigkeit unter Verwendung der gelehrten Methoden zu analysieren • Software unter Berücksichtigung von sicherheitstechnischen Standards und Normen zu entwickeln <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • wissen, dass technische Sicherheit in das technische System eingeplant werden muss. In der Planungsphase eines Softwareprojekts muss dabei dieser Aufwand berücksichtigt werden • können eigenständig vorhandene Normen und Standards in die Entwicklung des Softwareprojekts einbringen. • setzen die Implementierung von Software um mit Hilfe von gelehrten Muster und Methoden unter Berücksichtigung vorhandener Normen und Standards. • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • haben ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um Anwendungs- und Softwaresysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren • sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt • sind in der Lage Systeme sowie Anwendungen zu analysieren, entwerfen, entwickeln und pflegen, sodass sie den heutigen Maßstäben an die Sicherheit gerecht werden • 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 |
|--|--|

| | |
|--|--|
| Inhalt | <p>Vorlesung</p> <ul style="list-style-type: none"> • Grundlagen Fehler, Ausfälle, Risiko- und Zuverlässigkeitsanalyse, Sicherheitsfunktion, Sicherheitsintegritätslevel (SIL) • Modelle Risikomatrix, Risikograph, Markov Modell • Verfahren Fehlerbaumanalyse, Ereignisbaumanalyse, Zuverlässigkeitsanalyse • Lebenszyklus eines Steuer-/Regelsystems (S/R) • Sicherheitsfunktionen Planung der funktionalen Sicherheit, Bestimmung von SIL, Anforderungen und Entwurf von Hardware und Software sicherheitsbezogener elektrischer S/R-Systeme, Validierung des S/R-Systems. • Normen und Standards IEC 61508, Teile 1-7, Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer (E/E/PE) Systeme; IEC 62061 (Maschinenbereich), IEC 61511 (Prozessindustrie) • Anwendungsbeispiele SIL eines Prozessorsystems, einer Sicherheitsfunktion, eines Sicherheitsloops, Zuverlässigkeitsanalysen technischer Prozesse. <p>Praktikum</p> <ul style="list-style-type: none"> • Entwurf eines Regelungssystems für ein Fahrstuhl. Planung der Sicherheitsaspekte in das Regelungssystem unter Beachtung existierender Standards und Normen. Softwareentwurf des Regelungssystems unter Berücksichtigung von Sicherheitsaspekten. |
| Studien- /Prüfungsleistungen/ Prüfungsformen | Klausur: 90 min., benotet Laborarbeit, unbenotet |
| Medienformen | Vorlesung mit Beamer, Tafel, Skript physisch sowie digital (über Lernplattform), Übungen im Labor |
| Literatur | Börzsök, J.: Funktionale Sicherheit, VDE Verlag, 4. akt. Auflage, 2014. Halang, W.A.; Konakovsky, R.M.: Sicherheitsgerichtete Echtzeitsysteme, Springer Verlag, 2. Akt. Auflage, 2013 |

| | | | |
|--------------------------------------|--|---|---------------------|
| Modulbezeichnung | 22300 Software Engineering | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 22300 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Software Engineering | | |
| Studiensemester | 4 | | |
| Modulverantwortliche(r) | Prof. Dr. G. Nemirosvki | | |
| Dozent(in) | NN | | |
| Sprache | Deutsch (deutsches und englisches Literaturstudium erforderlich) | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 4 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung & Übungen: | 2 SWS, Gruppengröße max. 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 30h | 45h |
| | Summe: 75h (2,5 * 30 Std./ECTS) | 30h | 45h |
| Kreditpunkte (ECTS) | 2,5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 12000 Programmierung 1 14500 Programmierung 2 | | |
| Angestrebte Lernergebnisse | Kenntnisse Die Studierenden kennen <ul style="list-style-type: none"> • die wichtigsten Begriffe und Merkmale für einen professionellen Anforderungsanalyse • Modellierungssprachen im Hinblick auf die Dokumentation der Anforderungsanalyse • die Bedeutung und Wesensmerkmale einer qualitativ hochwertigen Software-Spezifikation | | |

| | |
|-----------------------------|--|
| | <p>Fertigkeiten</p> <p>Die Studierenden sind in der Lage,</p> <ul style="list-style-type: none"> Anforderungsanalysen unter Anleitung zu konzipieren, zu organisieren und durchzuführen, Anforderungen an Software-System auch bei Kunden und Benutzern zu eruieren, zu formulieren und deren Umsetzung zu überprüfen <p>Kompetenzen</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> Anforderungen an Software-Systeme auch von Nichtinformatikern ermitteln und kunden- und anwenderorientiert modellieren <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> haben ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um Anwendungs- und Softwaresysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren |
| Inhalt | <p>Vorlesung & Übungen</p> <ul style="list-style-type: none"> Vorgehens- und Prozessmodelle Requirements Engineering Software Arcjitektur und Design Patterns Software-Prüfung und -Qualitätssicherung Software Management Versionierungssysteme Einführung in Projektmanagement am Beispiel Scrum Software Wartung <p>Tools</p> <ul style="list-style-type: none"> Git MAven JUnit |
| Studien-/Prüfungsleistungen | Klausur 60 min., benotet |
| Medienformen | Vorlesung mit Beamer, Tafel, Skript physisch sowie digital (über Lernplattform), Übungen im Labor |
| Literatur | <p>Christine Rupp und die SOPHISTen, Requirements-Engineering und -Management: Aus der Praxis von klassisch bis agil, HANser Verlag, 2014, ISBN: 3446438939</p> <p>Jochen Ludewig, Horst Lichter, Software Engineering: Grundlagen, Menschen, Prozesse, Techniken, dpunkt Verlag, 2013, ISBN: 3864900921</p> <p>Robert C., Clean Coder: Verhaltensregeln für professionelle Programmierer, mitp, 2014, ISBN: 3826696956</p> |

| | |
|--|---|
| | <p>Hay, D.: Requirements Analysis: From Business Views to Architecture. Prentice Hall, 1st edition, 2011, ISBN-13: 978-0132762007</p> <p>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</p> <p>https://maven.apache.org/</p> <p>https://git-scm.com/</p> |
|--|---|

| | | | |
|---|---|-----------------------------|---------------------|
| Modulbezeichnung | 22500 Reverse Engineering | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 22500 | | |
| ggf. Untertitel | | | |
| Lehrveranstaltung | Vorlesung & Übungen Reverse Engineering | | |
| Studiensemester | 4 | | |
| Modulverantwortliche(r) | Prof. Dr. Martin Rieger | | |
| Dozent(in) | Prof. Dr. Martin Rieger | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 4 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung & Übungen: | 2 SWS, Gruppengröße bis 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 30 h | 45 h |
| | Summe: 75 h (2,5 * 30 Std./ECTS) | 30 h | 45 h |
| Kreditpunkte (ECTS) | 2,5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | Keine | | |
| Modulziele / Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden kennen</p> <ul style="list-style-type: none"> • Grundsätzliche Vorgehensweisen des Reverse Engineerings • Architektur x86, ARM • Assemblersprache • Windows: Prinzipien, Aufbau und Speicherbild von ausführbaren Programmen • Wirkungsweisen von Schadsoftware • Verschleierungstechniken von Schadsoftware | | |

| | |
|---|---|
| | <p>Fertigkeiten Die Studierenden können</p> <ul style="list-style-type: none"> • Mit Disassembler binären Code analysieren • Prozesse und Module analysieren • Im Speziellen Schadsoftware analysieren und dabei Methoden und Techniken des Reverse Engineering einsetzen. <p>Kompetenzen Die Studierenden sind fähig</p> <ul style="list-style-type: none"> • Grundlegende Kenntnisse über Konzepte und Methoden in Reverse Engineering umzusetzen • Reverse Engineering als ein integralen Bestandteil vieler forensischer Untersuchungen anzuwenden <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen • sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt • sind sich ihrer Verantwortung gegenüber Individuen und der Gesellschaft beim Umgang mit Sicherheitsrelevanten Informationen und Sicherheitsmethoden bewusst |
| <p>Inhalt</p> | <p>Vorlesung & Übungen</p> <ul style="list-style-type: none"> • Grundlagen der Analyse von Schadsoftware • Prozessorarchitekturen: X86, ARM • 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 • Programmier Techniken von Malware: Code-Verschleierung, Emulation, Erkennung von Virtualisierung oder Debuggern • Analyse von Schadsoftware für die Windows-Plattform |
| <p>Studien- /Prüfungsleistungen/ Prüfungsformen</p> | <p>Klausur (60 min): benotet</p> |

| | |
|--------------|---|
| Medienformen | Vorlesung mit Beamer; Skript in PDF-Format; Implementierung konkreter Anwendungsfälle und Visualisierung mit Beamer; Übungen und Tests in einem Labor |
| Literatur | 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 |

| | | | |
|--------------------------------------|--|-----------------------------|---------------------|
| Modulbezeichnung | 22600 Netzwerk- und Systemsicherheit | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 22600 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Netzwerk- und Systemsicherheit Praktikum Netzwerk- und Systemsicherheit | | |
| Studiensemester | 4 | | |
| Modulverantwortliche(r) | Prof. Dr. Tobias Heer | | |
| Dozent(in) | Prof. Dr. Tobias Heer | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 4 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung & Übungen: | 3 SWS, Gruppengröße bis 150 | |
| | Praktikum: | 1 SWS, Gruppengröße bis 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 45 h | 60 h |
| | Praktikum | 15 h | 30 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | Vorlesungen 15000 Betriebssysteme 21200 Netzwerke 12500 Einführung IT Security 13500 Kryptologie 1 Kenntnisse Die Studierenden kennen <ul style="list-style-type: none"> die Netzwerkprotokolle auf den verschiedenen Schichten des ISO/OSI Modells | | |

| | |
|---|---|
| | <ul style="list-style-type: none"> • die Grundlagen der Kryptographie • den Aufbau und die Funktion moderner Betriebssysteme |
| Modulziele / Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden kennen</p> <ul style="list-style-type: none"> • die Grundbegriffe der Sicherheit von IT Systemen und Netzwerken • historische und aktuelle Angriffe und Schwachstellen • verschiedene Angreifer-Typen und Angriffsmuster • typische Sicherheitsrisiken • die Gefahrenpotentiale und Sicherheitsmechanismen auf den verschiedenen Netzwerkschichten des ISO/OSI Modells (IPsec, TLS, 802.1x, RADIUS, Kerberos, OpenVPN, NATs und Firewalls) • Angriffsszenarien und Verteidigungsmöglichkeiten für Client und Server-Anwendungen • die Risiken und Funktionsweise von Single-Sign-On Systemen • die Wirkungsweise und Anwendung von Intrusion Detection Systemen und Honeypot Systemen <p>Fertigkeiten</p> <p>Die Studierenden sind in der Lage</p> <ul style="list-style-type: none"> • Adäquate Schutzmechanismen für Netzwerkkommunikation bestimmen • Firewall-Systeme basierend auf Anwendungsanforderungen konfigurieren • Schutzmechanismen für sichere Webkommunikation basierend auf TLS umsetzen • Sichere Kommunikationsarchitekturen erstellen und umsetzen • Sicherheitsrisiken in bestehenden Systemen und erkennen • gefährdete Anwendungen von anderen Anwendungen isolieren <p>Kompetenzen</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> • sich in die Rolle verschiedener Angreifer-Typen versetzen • Risiken in Systemen und Netzwerken einschätzen und diese vermeiden • Sicherheitsfunktionen in Netzwerk und auf Endgeräten einsetzen • Gefahren anhand von Systemereignissen und Log Einträgen erkennen und angemessen reagieren • können Unternehmensdaten extrahieren, konsolidieren und für die Auswertung in geeigneten Kennzahlensystemen bzw. für Recherche / Mustererkennung aufbereiten • 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 |

| | |
|---------------|---|
| | <ul style="list-style-type: none"> • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • haben praxisorientierte Kenntnisse der Wirtschaftswissenschaften und ein Grundverständnis für betriebliche Problemstellungen und der Methoden ihrer Beschreibung / Spezifikation und Beurteilung • können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen • verfügen über die zur Erfüllung von Anforderungen der Berufspraxis notwendigen persönlichen Kompetenzen: eigenverantwortliches Handeln, Zeitmanagement, Selbstorganisation • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben • sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt • sind in der Lage Systeme sowie Anwendungen zu analysieren, entwerfen, entwickeln und pflegen, sodass sie den heutigen Maßstäben an die Sicherheit gerecht werden <p>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</p> |
| <p>Inhalt</p> | <p>Vorlesung & Übungen</p> <ul style="list-style-type: none"> • Analyse historischer und aktueller Angriffe (Smurf, LAND, TLS Angriffe, etc.) • Anwendung der kryptografischen Grundlagen der Netzwerksicherheit (symmetrische und asymmetrische Verschlüsselung, Hash Funktionen, HMAC, Zertifikate, SSL/TLS, IPsec) • Sicherheitsziele in Netzwerk und IT Sicherheit • Sicherheitsmechanismen in Netzwerken auf den verschiedenen Netzwerkschichten (VPN, VLAN, NAC, Firewalls) |

| | |
|-----------------------------|---|
| | <ul style="list-style-type: none"> • Sicherheitsmechanismen in Betriebssystemen • E-Mail Sicherheit • Single-Sign-On Systeme • Intrusion Detection Systeme und Honeypots <p>Praktikum</p> <ul style="list-style-type: none"> • Aufsetzen sicherer Kommunikationssysteme • Konfiguration von Firewalls • Konfiguration sicherer Web-Kommunikation • Analyse und Einrichtung von Sicherheitsprotokollen in Netzwerken am Beispiel von OpenVPN und TLS • Erkennung von Veränderungen an Systemen • Systemhärtung und Anwendungsisolation • |
| Studien-/Prüfungsleistungen | Klausur 90 min., benotet Laborarbeit, unbenotet |
| Medienformen | <ul style="list-style-type: none"> • Vorlesung mit Beamer und Tafel, Lernmaterialien über Lernplattform, Übungen am Rechner |
| Literatur | <ul style="list-style-type: none"> • 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. |

| | | | |
|---|--|-----------------------------|---------------------|
| Modulbezeichnung | 22400 Cybersecurity | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 22400 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Seminar Cybersecurity Praktikum Cybersecurity | | |
| Studiensemester | 2 | | |
| Modulverantwortliche(r) | Prof. Holger Morgenstern | | |
| Dozent(in) | Prof. Holger Morgenstern | | |
| Sprache | Deutsch, bei Bedarf Englisch (muss vor Semesterbeginn geäußert werden), deutsches und englisches Literaturstudium erforderlich | | |
| Zuordnung zum Curriculum | Studiengang: | IT Security | |
| | Wahlrichtung: | - | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 4 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Vorlesung & Seminar: | 3 SWS, Gruppengröße bis 150 | |
| | Praktikum: | 1 SWS, Gruppengröße bis 20 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Seminar | 45 h | 60 h |
| | Praktikum | 15 h | 30 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 12500 Einführung IT Security 15500 Kryptologie 1 21400 Kryptologie 2 21200 Netzwerke | | |
| Modulziele / Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • Kennen die systematischen Grundlagen der IT Sicherheit in den Bereichen • Sicherheitsmanagement und Modelle • Identifikation, Authentifizierung, Authorisierung | | |

| | |
|--|--|
| | <ul style="list-style-type: none"> • Betriebssystem-, Datenbank-, Software- und Websicherheit <p>Fertigkeiten</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • Sind in der Lage die Grundlagen und Konzepte der IT Sicherheit in den behandelten Bereichen auf Fälle aus der Praxis anzuwenden, • Die Sicherheit von IT Systemen in den behandelten Bereichen systematisch zu untersuchen und zu bewerten, • Systematische IT Sicherheitskonzepte zu erstellen • Aktuelle Fragestellungen der IT Sicherheit wissenschaftlich zu untersuchen und zu präsentieren • Ethische Fragestellungen im Bereich der IT Sicherheit zu diskutieren und einzuschätzen <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • haben einen Überblick der Gesamtheit geschäftlicher Abläufe in mittelständischen Unternehmen (KMU) bis hin zum gehobenen Mittelstand („Hidden Champions“) <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • haben praxisorientierte Kenntnisse der Wirtschaftswissenschaften und ein Grundverständnis für betriebliche Problemstellungen und der Methoden ihrer Beschreibung / Spezifikation und Beurteilung • können sich und die Wirkung ihrer Person auf andere einschätzen und beweisen sich durch ihre adäquaten Mitarbeiterqualifikationen; beherrschen eine kooperative Teamarbeit in der sie Verantwortung tragen können und auch in widersprüchlichen Situationen tragfähige Entscheidungen treffen können • sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt • sind in der Lage Systeme sowie Anwendungen zu analysieren, entwerfen, entwickeln und pflegen, sodass sie den heutigen Maßstäben an die Sicherheit gerecht werden • 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 • sind sich ihrer Verantwortung gegenüber Individuen und der Gesellschaft beim Umgang mit Sicherheitsrelevanten Informationen und Sicherheitsmethoden bewusst |
|--|--|

| | |
|--|--|
| Inhalt | <p>Vorlesung, Seminar und Praktikum</p> <ul style="list-style-type: none"> • Sicherheitsmanagement • Identifikation und Authentifizierung • Zugriffskontrolle • Referenzmonitore • Betriebssystemsicherheit • Datenbanksicherheit • Softwaresicherheit • Sicherheitsmodelle • Websicherheit • Aktuelle Sicherheitsthemen • Cyber-Security-Ethics |
| Studien- /Prüfungsleistungen/ Prüfungsformen | Referat 20 min., benotet Laborarbeit, unbenotet |
| Medienformen | Vorlesung mit Beamer, Tafel, Skript physisch sowie digital (über Lernplattform) |
| Literatur | 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, 2010 Schwenk, J.: Sicherheit und Kryptographie im Internet, Springer, 2014 Eckert, C.: IT-Sicherheit, 9. Auflage, Oldenbourg Wissenschaftsverlag, München, 2014 |



Semester 5

| Modulbezeichnung | 23000 Projektmanagement | | | | | | | | | | | | | | | | | | |
|---|---|--------------------------|----------------|---------------------|-----------|-----|-----|------------|--|-----|---------------|--|-----|-------|--|--|---|-----|-----|
| ggf. Modulniveau | | | | | | | | | | | | | | | | | | | |
| ggf. Kürzel | 23000 | | | | | | | | | | | | | | | | | | |
| ggf. Untertitel | | | | | | | | | | | | | | | | | | | |
| ggf. Lehrveranstaltungen | Projektmanagement | | | | | | | | | | | | | | | | | | |
| Studiensemester | 5 | | | | | | | | | | | | | | | | | | |
| Modulverantwortliche(r) | Prof. Dr. Konrad R. Theobald, Prof. Dr. Otto Kurz | | | | | | | | | | | | | | | | | | |
| Dozent(in) | Prof. Dr. Konrad R. Theobald, Prof. Dr. Otto Kurz | | | | | | | | | | | | | | | | | | |
| Sprache | Deutsch (deutsches und englisches Literaturstudium erforderlich) | | | | | | | | | | | | | | | | | | |
| Zuordnung zum Curriculum | Studiengang: IT-Security, Technische Informatik, Wirtschaftsinformatik Studienschwerpunkt: alle Wahl/Pflicht: Pflichtmodul Semester: 5 Turnus: jedes Semester | | | | | | | | | | | | | | | | | | |
| Lehrform / SWS | Vorlesung, Fallstudie: 2 SWS, Gruppengröße max. 150 | | | | | | | | | | | | | | | | | | |
| Arbeitsaufwand | <table border="1"> <thead> <tr> <th><i>Veranstaltung/Art</i></th> <th><i>Präsenz</i></th> <th><i>Eigenstudium</i></th> </tr> </thead> <tbody> <tr> <td>Vorlesung</td> <td>30h</td> <td>10h</td> </tr> <tr> <td>Fallstudie</td> <td></td> <td>15h</td> </tr> <tr> <td>Studienarbeit</td> <td></td> <td>20h</td> </tr> <tr> <td colspan="3"><hr/></td> </tr> <tr> <td>Summe: 75h <i>(2,5 * 30 Std./ECTS)</i></td> <td>30h</td> <td>45h</td> </tr> </tbody> </table> | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> | Vorlesung | 30h | 10h | Fallstudie | | 15h | Studienarbeit | | 20h | <hr/> | | | Summe: 75h <i>(2,5 * 30 Std./ECTS)</i> | 30h | 45h |
| <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> | | | | | | | | | | | | | | | | | |
| Vorlesung | 30h | 10h | | | | | | | | | | | | | | | | | |
| Fallstudie | | 15h | | | | | | | | | | | | | | | | | |
| Studienarbeit | | 20h | | | | | | | | | | | | | | | | | |
| <hr/> | | | | | | | | | | | | | | | | | | | |
| Summe: 75h <i>(2,5 * 30 Std./ECTS)</i> | 30h | 45h | | | | | | | | | | | | | | | | | |
| Kreditpunkte (ECTS) | 2,5 | | | | | | | | | | | | | | | | | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | | | | | | | | | | | | | | | | | |
| Empfohlene Voraussetzungen | Sämtliche Module der ersten beiden Semester | | | | | | | | | | | | | | | | | | |
| Angestrebte Lernergebnisse | Kenntnisse Die Studierenden kennen <ul style="list-style-type: none"> • die wichtigsten Begriffe und Merkmale für professionelles Projektmanagement • Grundbegriffe der Geschäftsprozess-Modellierung • Verfahren zur Projektsteuerung • die Rollen der in Projekten tätigen Personen • wichtige Methoden von Software-Entwicklungsprozessen | | | | | | | | | | | | | | | | | | |

| | |
|--------|--|
| | <p>Fertigkeiten</p> <p>Die Studierenden sind in der Lage,</p> <ul style="list-style-type: none"> • Entwicklungsprozesse zu konzipieren und zu organisieren • eigene Arbeit in groben Zügen zu organisieren und selbständiges Arbeiten anzustreben <p>Kompetenzen</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> • die Verfügbarmachung von Produkten über den gesamten Prozess der Konzeptbildung, der Entwicklung, des Tests und der Abnahme bis zur Einführung innerhalb eines Teams dem Stand der Technik planen • Geschäftsprozesse modellieren <p>Das Modul trägt zum Erreichen der folgenden Kompetenzen bei:</p> <ul style="list-style-type: none"> • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • haben einen Überblick der Gesamtheit geschäftlicher Abläufe in mittelständischen Unternehmen (KMU) bis hin zum gehobenen Mittelstand („Hidden Champions“) • können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen • können sich und die Wirkung ihrer Person auf andere einschätzen und beweisen sich durch ihre adäquaten Mitarbeiterqualifikationen; beherrschen eine kooperative Teamarbeit in der sie Verantwortung tragen können und auch in widersprüchlichen Situationen tragfähige Entscheidungen treffen können |
| Inhalt | <p>Vorlesung</p> <p>Projektmanagement</p> <ul style="list-style-type: none"> • Grundlagen • Begründung der Notwendigkeit • Lebenszyklen und Phasenorientierung • Entwicklungsprozesse • Organisationsaufbau und Prozesssteuerung • Test- und Validierungsmethoden • Fallspezifische Prozessanpassung <p>Geschäftsprozessmodellierung</p> <ul style="list-style-type: none"> • Entwicklung einer Vision • Geschäftsvorschlag • Zielfixierung • Organisationsplanung und Rollenverteilung |

| | |
|-----------------------------|---|
| | <ul style="list-style-type: none"> • Geschäftsarchitektur und -modell • Risikoanalyse und -management <p>Fallstudie</p> <ul style="list-style-type: none"> • Entwicklung eines Geschäftsvorschlages • Planung eines Entwicklungsprozesses |
| Studien-/Prüfungsleistungen | Studienarbeit, benotet |
| Medienformen | <ul style="list-style-type: none"> • Multimediale Vorlesungspräsentation • Unterlagen über Internetpräsenz • Nutzung von diversen Applikationen • Fallstudie unter Nutzung von diversen Medien |
| Literatur | <p>Barnes, J.: Implementing the IBM Rational Unified Process and Solutions S: A Guide to Improving Your Software Development Capability and Maturity. Addison-Wesley Longman, 2007, ISBN-13: 978-0321369451</p> <p>Bohinc, T.: Grundlagen des Projektmanagements: Methoden, Techniken und Tools für Projektleiter. Gabal, 2010, ISBN-13: 978-3869361215</p> <p>Brugger, R.: Der IT Business Case: Kosten erfassen und analysieren - Nutzen erkennen und quantifizieren - Wirtschaftlichkeit nachweisen und realisieren. Springer, 2. Auflage, 2009, ISBN-13: 978-3540938576</p> <p>Kneuper, R.: CMMI: Improving Software and Systems Development Processes Using Capability Maturity Model Integration. Rocky Nook, 2008, ISBN-13: 978-1933952284</p> <p>Lessel, W.: Pocket Business: Projektmanagement: Projekte effizient planen und erfolgreich umsetzen. Cornelsen Verlag Scriptor, 3. Auflage, 2007, ISBN-13: 978-3589234066</p> <p>Liebig, M.: Entscheiden. Gabler, 1993, ISBN-13: 978-3409191784</p> <p>O'Regan, G.: Introduction to Software Process Improvement. Springer, 2010, ISBN-13: 978-0857291714</p> <p>Rupp, C.: Requirements-Engineering und -Management: Professionelle, iterative Anforderungsanalyse für die Praxis. Hanser Fachbuch, 5. Auflage, 2009, ISBN-13: 978-3446418417</p> <p>Versteegen, G.: Projektmanagement mit dem Rational Unified Process, Springer, 2008, ISBN: 978-3540667551</p> |

| | | | |
|---|---|---|---------------------|
| Modulbezeichnung | 23100 Unternehmenskonzepte / Digitale Fabrik | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Unternehmenskonzepte / Digitale Fabrik | | |
| Studiensemester | 5 | | |
| Modulverantwortliche(r) | Prof. Dr. Otto Kurz | | |
| Dozent(in) | Prof. Dr. Otto Kurz | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | Cyber Physical Systems | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 5 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung: | 4 SWS, Gruppengröße bis 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 60 h | 90 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 12000 Programmieren 1 | | |
| Modulziele / Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden kennen:</p> <ul style="list-style-type: none"> • die grundlegenden Komponenten der digitalen Fabrik, deren Eigenschaften und Anwendungsbereiche, sowie charakteristische Methoden der Konfiguration und Entwicklung. • Die grundlegenden Prinzipien der Betriebsorganisation und der Methoden zur Organisationsentwicklung (lernende Organisation). • Industrielle Prozessstrukturen und deren Wechselwirkung mit den internen und externen Komponenten der digitalen Fabrik. | | |

| | |
|--|--|
| | <ul style="list-style-type: none"> • Methoden zur Entwicklung komplexer virtueller Modelle zur Simulation und Erprobung der digitalen Fabrik. <p>Fertigkeiten</p> <p>Die Studierenden können:</p> <ul style="list-style-type: none"> • Betriebs- und Prozessstrukturen analysieren und darauf aufbauend optimierte Unternehmensabläufe planen und realisieren. • Komponenten der digitalen Fabrik auswählen und zielgerichtet zur Produktivitätssteigerung einsetzen oder vorhandene Strukturen in diesem Sinne entwickeln und optimieren. • Konzepte entwickeln um bei kürzeren Innovationszyklen, kleineren Stückzahlen, hohen Anforderungen an Produktsicherheit und Produktqualität und häufigen Produktänderungen die Prozesse dennoch sicher zu beherrschen. • Komplexe Netzwerke, Interaktionen, Kommunikation, Datenaustausch, etc. für die flexiblen Komponenten der digitalen Fabrik planen und realisieren. <p>Kompetenzen</p> <p>Die Studierenden sind fähig:</p> <ul style="list-style-type: none"> • Logisch und abstrakt zu denken. • die Praxisrelevanz der erlernten Methoden und Prinzipien zu erkennen und diese zielgerichtet zur Lösung von Ingenieurproblemen anzuwenden. • Technisch/organisatorische Prozesse unter Anwendung flexibler Rechnersysteme zu erfassen, die Lösungsmethoden auszuwählen und Systeme zu modellieren. • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams • sind in der Lage, die Planung, den Entwurf, die Implementierung und den Betrieb von Hardware/Software-Systemen wirkungsvoll zu unterstützen • sind in der Lage, den in den technischen Anwendungsbereichen der Informatik statt-findenden und sich kontinuierlich verstärkenden Einzug von Informationstechnologie wirkungsvoll zu unterstützen und aktuelle Trendthemen der IT (z.B. „Internet der Dinge“, „Industrie 4.0“, „Elektro-mobilität“, „Energiewende“) in die praktische Anwendung zu überführen • sind in der Lage, Kunden bei der Planung und Auswahl sowie beim Betrieb und Management komplexer und sicherer Informatiklösungen zur Optimierung von Produktions- und Arbeitsabläufen in Unternehmen zu beraten und zu unterstützen. Sie können geeignete Schulungskonzepte entwickeln und Schulungen und Unterweisungen durchführen |
|--|--|

| | |
|--|---|
| | <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • haben ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um Anwendungs- und Softwaresysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in Bezug auf einen bestimmten Anwendungsbedarf zu verfolgen • verfügen über die zur Erfüllung von Anforderungen der Berufspraxis notwendigen persönlichen Kompetenzen: eigenverantwortliches Handeln, Zeitmanagement, Selbstorganisation • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben |
| Inhalt | <p>Vorlesung & Übungen</p> <ul style="list-style-type: none"> • Vertiefen und festigen der Grundkenntnisse zur Optimierung von Unternehmensabläufen und Komponenten in der digitalen Fabrik. • Komplexe Sachverhalte erfassen und unter Beachtung übergeordneter Randbedingungen geeignete Lösungswege finden und bewerten. • Kennenlernen der grundlegenden Komponenten der digitalen Fabrik, d.h. Steuerungen für Maschinen und Anlagen, flexible Handhabungsgeräte, Sensoren und Aktoren, Netzwerke, Informations- und Kommunikationssysteme, ERP-Systeme und Logistik, Bild- und Signalverarbeitung, VR-Systeme, etc.. • Methoden um Planungsprozesse zu beschleunigen, zu sichern und Kosten zu senken. • Vermeidung von Planungsfehlern und Prozesssicherung durch geeignete Simulationsverfahren. • Methoden zur Entwicklung und 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 Modellen. • Anpassung der Betriebsorganisation an die Erfordernisse der digitalen Fabrik, lernende und selbstoptimierende Organisation. • Anforderungen an die IT-Sicherheit der digitalen Fabrik. • Kenngrößen zur Bewertung der digitalen Fabrik. |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur, 90 Minuten, benotet |

| | |
|--------------|--|
| Medienformen | Beamer + Sympodium, Tafel, Skripte und Übungsaufgaben sind als PDF-File oder Excell-Tabellen online im Intranet verfügbar. |
| Literatur | <p>VDI-Richtlinie 4499, Blatt 1: Digitale Fabrik – Grundlagen, VDI-Gesellschaft Fördertechnik Materialfluss Logistik, 2008.</p> <p>Kühn, W.: Digitale Fabrik. Fabriksimulation für Produktionsplaner, Hanser Verlag, München.</p> <p>Westkämper, E.: Digitale Produktion, Springer Verlag, Berlin, New York.</p> <p>Bracht, U.; Geckler, D.; Wenzel, S.: Digitale Fabrik. Methoden und Praxisbeispiele, Springer Verlag, Berlin, New York.</p> <p>Hehenberger, P [u.a.]: Computerunterstützte Fertigung, Eine kompakte Einführung. 1. Aufl.: Springer Verlag, Berlin, New York.</p> <p>Schack, R.: Methodik zur bewertungsorientierten Skalierung der Digitalen Fabrik, Herbert Utz Verlag, München.</p> <p>Bullinger, H.-J.: Einführung in das Technologiemanagement, B.G. Teubner Verlag, Stuttgart.</p> |

| | | | |
|---|---|---|---------------------|
| Modulbezeichnung | 23200 Verteilte Systeme (Technik) | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Verteilte Systeme (Technik) Praktikum Verteilte Systeme (Technik) | | |
| Studiensemester | 5 | | |
| Modulverantwortliche(r) | Prof. Dr. Derk Rembold | | |
| Dozent(in) | Prof. Dr. Derk Rembold | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | Cyber-Physical-Systems | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 5 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung & Übungen: | 3 SWS, Gruppengröße bis 150 | |
| | Praktikum: | 1 SWS, Gruppengröße bis 20 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 45 h | 30 h |
| | Praktikum | 15 h | 60 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 12000 Programmieren 1 | | |
| Modulziele / Angestrebte Lernergebnisse | Kenntnisse Die Studierenden <ul style="list-style-type: none"> kennen Verteilte Systeme (Technik) mit Schwerpunkten in der Automatisierungstechnik und in den Fahrzeugen kennen die Architekturen, Botschaften und Zeitverhalten verteilter Systeme behandelt | | |

| | |
|--|--|
| | <p>Fertigkeiten</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können den Entwurfes und die Realisierung der verteilten Systeme <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind in die Lage, vernetzte technische Systeme zu analysieren, entwerfen und aufzubauen • sind in der Lage, praxisgerechte und kostengünstige Kundenlösungen, darunter intelligente vernetzte Geräte, für Industrie und Wirtschaft, insbesondere mit Schwerpunkten in der Informations-, Kommunikations- und Softwaretechnik, der Automobilelektronik/ –informatik zu entwickeln • beherrschen wichtige Anwendungen der Technischen Informatik (Simulationstechnik Bildverarbeitung, Automobilanwendungen, Robotik, Mobile Computing / Cloud Computing) und können diese für allgemeine und spezielle Anwendungen weiterentwickeln und optimieren • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams • sind in der Lage, den in den technischen Anwendungsbereichen der Informatik statt-findenden und sich kontinuierlich verstärkenden Einzug von Informations-technologie wirkungsvoll zu unterstützen und aktuelle Trendthemen der IT (z.B. „Internet der Dinge“, „Industrie 4.0“, „Elektro-mobilität“, „Energiewende“) in die praktische Anwendung zu überführen • sind in der Lage, die Planung, den Entwurf, die Implementierung und den Betrieb von Hardware/Software-Systemen wirkungsvoll zu unterstützen • sind in der Lage, Kunden bei der Planung und Auswahl sowie beim Betrieb und Management komplexer und sicherer Informatiklösungen zur Optimierung von Produktions- und Arbeitsabläufen in Unternehmen zu beraten und zu unterstützen. Sie können geeignete Schulungskonzepte entwickeln und Schulungen und Unterweisungen durchführen. • 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 |
|--|--|

| | |
|--|---|
| | <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in Bezug auf einen bestimmten Anwendungsbedarf zu verfolgen • verfügen über die zur Erfüllung von Anforderungen der Berufspraxis notwendigen persönlichen Kompetenzen: eigen-verantwortliches Handeln, Zeitmanagement, Selbstorganisation • Sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben |
| Inhalt | <p>Vorlesung & Übungen</p> <ul style="list-style-type: none"> • Einführung: Technischer Prozess, Automatisierungsfunktionen, Sprachen und Notationen, Softwaremuster. • Softwaremuster für verteilte Systeme: Einsatz, Struktur, Verhalten, Entwurf, Konstruktion, Varianten der Muster Client-Dispatcher-Server, Forward-Receiver, Communicator, Proxy, Observer, Layers, Broker, Model-View-Controller. • Vernetzte Systeme in Fahrzeugen: CAN: Protokoll, Kommunikationsmatrix, Botschaften, Signale, CAPL; LIN: Protokoll, Architektur, Botschaften, Schedule, LDF Beschreibungssprache, FlexRay: TDMA-Verfahren, Botschaften, In-Cycle Steuerung, Zeitsynchronisation, Busguardian. • Busse in der Automatisierungstechnik: ProfiBus: Betriebsarten, Telegramme, Dienste, Zeitverhalten; ProfiNet: Real-Time-, Isochrone Real-Time-Kommunikation, AD-i: Übertragungsmedium, Telegramme; CANopen; SafetyBusP: sicherheitsgerichtete Maßnahmen • Testen verteilter Systeme: Testobjekte, Testplanung, Testausführung, Testauswertung, Protokollanalyse, Informationsflussverfolgung, Zeitsynchronisation, Datenhaltung <p>Praktikum</p> <ul style="list-style-type: none"> • Realisierung des Client-Dispatcher-Server Musters • Ereignisbeobachtung über ein Netzwerk / Zeitsynchronisation • Simulation, Entwurf und Realisierung von CAN Netzwerken |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur 90min., benotet Laborarbeit, unbenotet |

| | |
|--------------|--|
| Medienformen | Tafel, Teilskript, Übungsblätter, Overhead, PC mit Beamer, Intranet- und Internetzugriff |
| Literatur | Buschmann, F. u.a.: Pattern - Oriented Software Architecture: A System of Patterns; John Wiley & Sons. Wörn, H.; Brinkschulte, U.: Echtzeitsysteme, Springer. Zimmermann, W.; Schmidgall, R.: Bussysteme in der Fahrzeugtechnik, Protokolle und Standards, 2. Vieweg. Reißenweber, B.: Feldebussysteme zur industriellen Kommunikation, Oldenbourg Industrieverlag München. |

| | | | |
|--------------------------------------|--|---|---------------------|
| Modulbezeichnung | 23300 Intelligente Lernende Systeme | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | ILS | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Intelligente Lernende Systeme Praktikum Intelligente Lernende Systeme | | |
| Studiensemester | 5 | | |
| Modulverantwortliche(r) | Prof. Dr. A Knoblauch | | |
| Dozent(in) | Prof. Dr. Andreas Knoblauch, Prof. Dr. Walter Hower | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik Wirtschaftsinformatik | |
| | Wahlrichtung: | Cyber-Physical-Systems | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 5 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | 23310 Vorlesung: 3 SWS, Gruppengröße bis 150 23320 Praktikum: 1 SWS, Gruppengröße bis 20 | | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | 23310 Vorlesung | 45 h | 60 h |
| | 23320 Praktikum | 15 h | 30 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | 11000 Mathematik 1 14000 Mathematik 2 15500 Algorithmik | | |
| Empfohlene Voraussetzungen | Grundlagenwissen in Mathematik und Algorithmik | | |
| Angestrebte Lernergebnisse | Kenntnisse Die Studierenden kennen | | |

- die wesentlichen Grundlagen der Künstlichen Intelligenz, insbesondere intelligente Agenten, Neuronale Netze und Maschinelles Lernen
- wesentliche Methoden des maschinellen Lernens und deren Bedeutung für die Entwicklung intelligenter lernender Systeme, insbesondere im Bereich Cyber-Physical-Systems und IT-Security
- Architekturen von technischen und biologischen intelligenten Systemen

Fertigkeiten

Die Studierenden können

- die Eignung von Algorithmen zur Lösung eines gegebenen Planungs-, Erkennungs- oder Lernproblems einschätzen
- intelligente Systeme zur Lösung eines gegebenen Planungs-, Erkennungs- oder Lernproblems entwerfen, indem sie geeignete Methoden und Algorithmen der Künstlichen Intelligenz und des maschinellen Lernens auswählen und anpassen.
- wesentliche Methoden der Künstlichen Intelligenz und des maschinellen Lernens anwenden und mit Hilfe von Matlab und/oder Python/Numpy/Scikit-learn implementieren

Kompetenzen

Die Studierenden

- sind fähig, die Möglichkeiten und Grenzen von Künstlicher Intelligenz und Maschinellem Lernen einzuschätzen
- sind fähig, geeignete Verfahren des maschinellen Lernens zur Lösung technischer Probleme, insbesondere im Bereich Cyber-Physical-Systems und IT-Security auszuwählen und sie in intelligenten Systemen zu realisieren.
- können Unternehmensdaten extrahieren, konsolidieren und für die Auswertung in geeigneten Kennzahlensystemen bzw. für Recherche /Mustererkennung aufbereiten
- haben ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um Anwendungs- und Softwaresysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren
- können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen
- sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben
- 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

| | |
|--|---|
| | <ul style="list-style-type: none"> • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams • sind in der Lage, die Planung, den Entwurf, die Implementierung und den Betrieb von Hardware/Software-Systemen wirkungsvoll zu unterstützen • sind in der Lage, den in den technischen Anwendungsbereichen der Informatik stattfindenden und sich kontinuierlich verstärkenden Einzug von Informations-technologie wirkungsvoll zu unterstützen und aktuelle Trendthemen der IT (z.B. „Internet der Dinge“, „Industrie 4.0“, „Elektromobilität“, „Energiewende“) in die praktische Anwendung zu überführen <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • haben ein fundiertes Methoden- und Fachwissen aus der Informatik, um betriebliche Anwendungssysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen. • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben. |
| Inhalt | <p>Vorlesungen, Übung und Praktikum:</p> <ul style="list-style-type: none"> • Intelligente Steuerung und Planung: Methoden aus der Künstlichen Intelligenz, Modelle von Intelligenten Agenten, Diskrete Zustandsraumbeschreibung, A*-Algorithmus, Dynamisches Programmieren, Reinforcement Learning, Grundlagen des Autonomen Lernen von Zustandsräumen und Situationserkennern • Methoden des Maschinellen Lernens: Lineare Modelle für Regression und Klassifikation, Neuronale Netze, Kernel Methoden, Graphical Models, Probabilistische Inferenz, K-means, Mixtures of Gaussians, Kalman Filter • Kognitive Architekturen: Technische und biologische Systeme • Implementierung ausgewählter Algorithmen mit Python/Numpy/Scikit-learn und Anwendung auf Daten aus dem Bereich Cyber-Physical-Systems, IT-Security und Wirtschaft. |
| Studien-/Prüfungsleistungen/ Prüfungsformen | <p>Modul ILS: Klausur 90 min, benotet</p> <p>Praktikum ILS: Praktische Arbeit, unbenotet</p> |

| | |
|--------------|--|
| Medienformen | Vorlesung mit Beamer; Teil-Skript in PDF-Format; Implementierung konkreter Anwendungsfälle und Visualisierung mit Beamer; Übungen und Tests in einem Labor |
| Literatur | 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. |

| | | | |
|--------------------------------------|--|--|---------------------|
| Modulbezeichnung | 23410 Medieninformatik | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 23410 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung Medieninformatik Projekt Medieninformatik | | |
| Studiensemester | 5 | | |
| Modulverantwortliche(r) | Prof. Dr. Konrad R. Theobald | | |
| Dozent(in) | Prof. Dr. Konrad R. Theobald | | |
| Sprache | Deutsch (deutsches und englisches Literaturstudium erforderlich) | | |
| Zuordnung zum Curriculum | Studiengang: | Wirtschaftsinformatik | |
| | Wahlrichtungen: | alle | |
| | Wahl/Pflicht: | Wahlpflichtmodul | |
| | Semester: | 5 | |
| | Turnus: | jedes Semester (falls Wahlpflichtmodul zustande kommt) | |
| Lehrform / SWS | Vorlesung: | 2 SWS, Gruppengröße max. 150 | |
| | Projekt: | 2 SWS, Gruppengröße max. 20 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung | 30h | 20h |
| | Projekt | 30h | 70h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60h | 90h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 11500 Einführung in die Informatik 15500 Algorithmik | | |
| Angestrebte Lernergebnisse | Kenntnisse Die Studierenden kennen <ul style="list-style-type: none"> • die wichtigsten Medienformen und deren Speicherung in digitalen Medien • digitale Bearbeitungssysteme für digitale Medien und deren Leistungsfähigkeit | | |

| | |
|---------------|--|
| | <ul style="list-style-type: none"> • die Wirkung von Medien auf Individuen und die Wichtigkeit der multimodalen Verknüpfung • elektronische und klassische Medienmärkte <p>Fertigkeiten</p> <p>Die Studierenden sind in der Lage,</p> <ul style="list-style-type: none"> • Medien mit professionellen Geräten aufnehmen • Erstellte Medien am Computer digital bearbeiten • Geschäftsvorschläge für die Medienbranche zu entwickeln und zu vertreten • Medienprojekte verantwortlich zu betreiben <p>Kompetenzen</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> • die Entwicklung von diversen Medien von der Idee bis zur Verfügbarmachung beim Rezipienten konzipieren, planen und umsetzen • den Einsatz von Medien zur Unterstützung und Optimierung von Aufgaben im gesamten Bereich der Wirtschaftsinformatik zu erkennen und anzuwenden <p>Das Modul trägt zum Erreichen der folgenden Kompetenzen bei:</p> <ul style="list-style-type: none"> • sind in der Lage, übergreifende Prozesse zwischen Wirtschaftseinheiten (Unternehmen, Verwaltungseinheiten) durch Anwendungssoftware zu unterstützen • verfügen über Kenntnisse zur Konzeption neuer Geschäftsmodelle, die auf modernen Informations- und Kommunikationstechnologien beruhen (E-Business, Mobile-Business, Industrie 4.0) • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen |
| <p>Inhalt</p> | <p>Vorlesung:</p> <ul style="list-style-type: none"> • Wirkung von Medien auf das Individuum • Mediale Basiselemente (Art, Produktion, Bearbeitung, komprimierte Speicherung und Verwendung) <ul style="list-style-type: none"> ○ Bilder ○ Animationen ○ Audio ○ Video ○ Computerspiele • Einsatz von Medien innerhalb und außerhalb des Webs • Nutzung der Multimodalität • Verfügbarmachen von Medien in elektronischen und klassischen Märkten |

| | |
|-----------------------------|--|
| | <p>Projekt:</p> <ul style="list-style-type: none"> • Entwicklung eines qualifizierten Geschäftsvorschlags für die anstehende Projektarbeit inklusive einer Marktanalyse • Sichtung, Bewertung und Auswahl des durchzuführenden Projekts • Projektplanung (Aufgaben, Netzplan, Meilensteine) und Arbeitsverteilung (Rollen, Verantwortlichkeiten, Mitarbeit) • Herstellung eines kleineren Medienproduktes |
| Studien-/Prüfungsleistungen | 23400 Praktische Arbeiten, benotet |
| Medienformen | <ul style="list-style-type: none"> • Multimediale Vorlesungspräsentation • Unterlagen über Internetpräsenz • Nutzung von diversen Applikationen • Projekt unter Nutzung von diversen Medien |
| Literatur | <p>Altendorfer, O.: Mediensystem der Bundesrepublik Deutschland, Band 1 und 2. VS Verlag für Sozialwissenschaften, 2001 & 2004, ISBN-13: 978-3531134352 & 978-3531134369</p> <p>Altmann, R.: Insiderbuch Digitale Fotografie und Bildbearbeitung, Band 1 und 2. Midas, 2001 & 2003 ISBN-13: 978-3907020845 & 978-3907020647</p> <p>Bär, M. et al.: Digitaler Videoschnitt. bhv, 2000, ISBN-13: 978-3826686153</p> <p>Bender, M., Brill, M.: Computergrafik: Ein anwendungsorientiertes Lehrbuch. Hanser Fachbuchverlag, 2005, ISBN-13: 978-3446404342</p> <p>Böhringer, J., Bühler, P., Schlaich, P.: Kompendium der Mediengestaltung - Konzeption und Gestaltung für Digital- und Printmedien. Springer, 4. Auflage, 2008, ISBN-13: 978-3540785255</p> <p>Büchle, F.: Digitales Filmen: Einfach gute Videofilme drehen und nachbearbeiten. Galileo Press, 2. Auflage, ISBN-13: 978-3898426527</p> <p>Butz, A. et al.: Medieninformatik: Eine Einführung. Pearson Studium, 2009, ISBN-13: 978-3827373533</p> <p>Goldberg, R.E., Bosi, M.: Introduction to Digital Audio Coding and Standards. Springer Netherlands, 2002, ISBN-13: 978-1402073571</p> <p>Harrington, R., Weiser, M.: Producing Video Podcasts. Producing Video Podcasts: A Guide for Media Professionals. Butterworth Heinemann, 2008, ISBN-13: 978-0240810294</p> <p>Henning, P. A.: Taschenbuch der Medieninformatik. Hanser Fachbuch, 2005, ISBN-13: 978-3446402997</p> <p>Henning, P. A.: Taschenbuch Multimedia. Hanser Fachbuch, 4. Auflage, 2007, ISBN-13: 978-3446409712</p> |

| | |
|--|--|
| | <p>Holzinger, A.: Basiswissen Multimedia, Band 1 - 3. Vogel Business Media, 2000-2002, ISBN-13: 978-3802319143 (2. Auflage), 978-3834332073, 978-3802318580</p> <p>Klimsa, P., Krömker, H.: Handbuch Medienproduktion. VS Verlag für Sozialwissenschaften, 2005, ISBN-13: 978-3531140315</p> <p>McShaffry, M.: Game Coding Complete. Cengage Learning Services, 3. Auflage, 2009, ISBN-13: 978-1584506805</p> <p>D. Mühlbacher et al.: Computerspiele - Design und Programmierung. mitp, 2. Auflage, 2003, ISBN-13: 978-3826609206</p> <p>Poynton, C.: Digital Video and HDTV Algorithms and Interfaces. Morgan Kaufmann, 2001, ISBN-13: 978-1558607927</p> <p>Reil, A.A.: Videofilme - professionell gemacht: Kalkulation - Ausstattung - Ideen - Tipps. Dpunkt Verlag/Edition Mediabook, 2. Auflage, 2008, ISBN-13: 978-3898645454</p> <p>Rogge, A.: Die Videoschnitt-Schule: Tipps und Tricks für spannendere und überzeugendere Filme. Galileo Design, 3. Auflage, 2009, ISBN-13: 978-3836215114</p> <p>Schmidt, U.: Digitale Film- und Videotechnik. Hanser Fachbuchverlag, 3. Auflage, 2010, ISBN-13: 978-3446424777</p> <p>Stapelkamp, T.: DVD-Produktionen gestalten erstellen nutzen - Video interaktiv: DVD, Blu-ray Disc, HD DVD. Audio-/Videotechnik: DVD-Formate, TV, Podcast. Springer, 2007, ISBN-13: 978-3540331308</p> <p>Steinke, L.: Spieleprogrammierung. bhv, 2. Auflage, 2008, ISBN-13: 978-3826681622</p> |
|--|--|

| | | | |
|--------------------------------------|---|-----------------------------|---------------------|
| Modulbezeichnung | 23500 Projektstudium | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 23500 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Projektstudium Projekt Projekt Studium Seminar | | |
| Studiensemester | 5 | | |
| Modulverantwortliche(r) | Prof. Dr. German Nemirovski | | |
| Dozent(in) | Professoren der Fakultät | | |
| Sprache | Deutsch und/oder Englisch | | |
| Zuordnung zum Curriculum | Studiengang: | IT Security | |
| | Wahlrichtungen: | alle | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 5 | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Projekt: | 2 SWS, Gruppengröße bis 20 | |
| | Seminar: | 2 SWS, Gruppengröße max. 20 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Projekt | 30h | 120h |
| | Seminar | 60h | 15h |
| | Summe: 225h <i>(7,5 * 30 Std./ECTS)</i> | 90h | 135h |
| Kreditpunkte (ECTS) | 7,5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | Je nach Projektausrichtung alle Module der ersten 4 Semester | | |
| Angestrebte Lernergebnisse | Kenntnisse Die Studierenden kennen <ul style="list-style-type: none"> • Methoden des Projektmanagements und • die fortgeschrittenen kryptografischen Algorithmen oder • die fortgeschrittenen Techniken der Netzwerkssicherheit oder • die fortgeschrittenen Techniken der Sicherheit von eingebetteten -Systemen | | |

| | |
|--|--|
| | <p>Fertigkeiten</p> <p>Die Studierenden sind in der Lage,</p> <ul style="list-style-type: none"> • können die selbständig erlernten Algorithmen bzw. Techniken anwenden, um systematisch reale Probleme aus dem Studienbereich zu analysieren und im Team zu lösen • können die Projektergebnisse dokumentieren und präsentieren <p>Kompetenzen</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> • Methoden des Projektmanagements umsetzen und dabei die besonderen Aspekte in der Informatik berücksichtigen • komplexe Probleme erkennen, spezifizieren und lösen • Wissen, Methoden und Konzepte problembezogen übertragen • systematisch Probleme aus dem Studienbereich analysieren und mit wissenschaftlichen Methoden Probleme lösen • Sachzusammenhänge auf das Wesentliche abstrahieren • eigene Arbeit termintreu organisieren und eigenverantwortlich voran zu treiben • komplexe Sachverhalte strukturieren, visualisieren, präsentieren • wichtige eintretende Ereignisse erkennen und bewerten • ihre eigenen Leistungen bewerten und sich kritisch hinterfragen • zielgerichtet eine fachliche Recherche durchführen <p>Das Modul trägt – teilweise je nach Themenauswahl - zum Erreichen der folgenden Kompetenzen bei:</p> <ul style="list-style-type: none"> • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen • können sich und die Wirkung ihrer Person auf andere einschätzen und beweisen sich durch ihre adäquaten Mitarbeiterqualifikationen; beherrschen eine kooperative Teamarbeit in der sie Verantwortung tragen können und auch in widersprüchlichen Situationen tragfähige Entscheidungen treffen können • sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt • sind in der Lage Systeme sowie Anwendungen zu analysieren, entwerfen, entwickeln und pflegen, sodass sie den heutigen Sicherheits-Maßstäben gerecht werden |
|--|--|

| | |
|-----------------------------|---|
| | <ul style="list-style-type: none"> • 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 |
| Inhalt | <ul style="list-style-type: none"> • Eigenständige Bearbeitung eines realen Problems aus dem Studienbereich von der Problemanalyse bis zur marktfähigen Lösung im Projektteam • Coaching des Projektteams durch den Dozenten und Mitarbeiter |
| Studien-/Prüfungsleistungen | <p>Praktische Arbeiten, benotet</p> <p>Hausarbeit, benotet</p> |
| Medienformen | <ul style="list-style-type: none"> • Nutzung von diversen Applikationen • Nutzung von diverser Medien • Projektarbeitsplatz |
| Literatur | <p>Hindel, B. et al.: Basiswissen Software Projektmanagement. Dpunkt ISBN 3898642305</p> <p>Katzenbach, J. R., Smith, D. K.: The Wisdom of Teams. Creating the High-Performance Organization. Harvard Business School Press, ISBN 0875843670</p> <p>Lessel, W.: Projektmanagement, Cornelsen, ISBN 3589219033</p> <p>Schreckeneder, B. C.: Projektcontrolling. Projekte über-wachen, bewerten, präsentieren. Haufe, ISBN 344805349X</p> <p>Weitere projektspezifische Literatur wird vom Dozenten zum Beginn des Projekts benannt bzw. von den Studierenden ermittelt</p> |

| | | | |
|--------------------------------------|---|---|---------------------|
| Modulbezeichnung | 23600 Datenbanken 2 | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 23600 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Datenbanken 2 | | |
| Studiensemester | 5 | | |
| Modulverantwortliche(r) | Prof. Dr. Jörg Röhrle | | |
| Dozent(in) | Prof. Dr. Jörg Röhrle | | |
| Sprache | Deutsch, bei Bedarf Englisch (muss vor Semesterbeginn geäußert werden) | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | Application Development | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 5 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung & Übungen: | 4 SWS, Gruppengröße bis 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 60 h | 90 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | <p>Profunde Kenntnisse auf dem Bereich der Datenbanksysteme, der prozeduralen und objektorientierten Programmierung auf der Basis der Programmiersprache Java, sowie der Betriebssysteme und Netzwerke, konkret Module</p> <p>12000 / 14500 Programmieren I und II 21000 Datenbanken I 15000 Betriebssysteme und Netzwerke I 22000 Webbasierte Anwendungen 21100 BWL und Management</p> | | |

| | |
|---------------------------------------|--|
| <p>Angestrebte Lernergebnisse</p> | <p>Kenntnisse Die Studierenden kennen</p> <ul style="list-style-type: none"> • die Implementierungstechniken zur Formulierung komplexer Anfragen auf Basis eines (objekt-) relationalen Datenbanksystems in SQL • 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 grundlegenden Techniken der Datenmodellierung für komplexe Anwendungsbereiche aus dem Gebiet der Informatik • die „Themenorientierung“ im Hinblick auf die Auswertung komplexer Auswertungen sowie deren Abgrenzung zur Prozessorientiertheit operativer Aufgaben • die Prinzipien spaltenorientierter (In-Memory) Datenbanksysteme • den prinzipiellen Aufbau von JEE-Applikationsservern <p>Fertigkeiten Die Studierenden sind in der Lage</p> <ul style="list-style-type: none"> • ein Datenmodell für Datawarehouse-Anwendungen zu konzipieren • komplexe Datenbankanfragen auf Basis des (objekt-) relationalen Datenmodells zur Entscheidungsunterstützung in Bereichen des Controlling oder der Strategischen Unternehmensführung zu formulieren • mehrdimensionale Wissensbasen im Sinne einer OLAP - Architektur (Online Analytical Processing) aufzubauen • einfache und komplexe Zusammenhänge zu Unternehmensdaten im Sinne eines Business Analytics zu bewerten • Einsatzaspekte spaltenorientierte Datenbanksysteme zu bewerten • Die Persistenzsicherung vermittels JEE-Applikationen zu realisieren <p>Kompetenzen Die Studierenden sind fähig</p> <ul style="list-style-type: none"> • 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 • eine Einordnung von Business Intelligence in die Unternehmens-IT vorzunehmen • eine Data Warehouse-Anwendung auf Basis eines Serverdatenbanksystems zu konzipieren und einzusetzen • den Integrationsprozess für große, unterschiedlich strukturierte und verteilte Datenbasen hin zu einer vereinheitlichten Datenbasis für komplexe, mehrdimensionale Auswertungen vorzunehmen • die wichtigsten Technologien für die Wissensgewinnung aus multidimensionalen Daten anzuwenden • einfachere JEE-Applikationen zu konzipieren |
|---------------------------------------|--|

| | |
|---|---|
| | <ul style="list-style-type: none"> • Einsatzaspekte spaltenorientierter Datenbanksysteme zu bewerten. <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse Die Studierenden</p> <ul style="list-style-type: none"> • sind in der Lage, übergreifende Prozesse zwischen Wirtschaftseinheiten (Unternehmen, Verwaltungseinheiten) durch Anwendungssoftware zu unterstützen • haben ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um betriebliche Anwendungssysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren • haben einen Überblick der Gesamtheit geschäftlicher Abläufe, insbesondere in kleineren mittelständischen Unternehmen • können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; leben bewusst, nehmen Ereignisse wahr, können diese einschätzen und ihre Kenntnisse und Erfahrungen zur selbständigen Lösung dieser Aufgaben transferieren; kennen die zwischenmenschlichen Umgangsformen und zeigen ein diesbezüglich diszipliniertes Verhalten; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben |
| <p>Inhalt</p> | <p>Vorlesung & Übungen</p> <ul style="list-style-type: none"> • Bewertung operativer und analytischer Datenbanken • Konzeption von Datenmodell für Data Warehouses • Nutzung von Metadaten für die Verwendung in einem Data Warehouse • Aufbereitung von Daten zur Nutzung in einem Data Warehouse • Anwendung von Optimierungstechniken für sehr große Datenbanken • Anwendung multidimensionaler Auswertungen • Aufbau von Data Marts nach anwendungsrelevanten Kriterien • Datenverdichtungen im Sinne eines Data Mining vorzunehmen • Bereitstellung von Information zur Transparenzmachung von Geschäftsprozessen • Konzept und Realisierung von Anfragen auf Basis spaltenorientierter Datenbanksysteme • Konzept und Realisierung von JEE-Applikationen |
| <p>Studien- /Prüfungsleistungen/ Prüfungsformen</p> | <p>mündliche Prüfung, benotet</p> |
| <p>Medienformen</p> | <p>Vorlesung mit Beamer; Skript in PDF-Format; Implementierung konkreter Anwendungsfälle und Visualisierung mit Beamer; Übungen und Tests in einem Labor</p> |
| <p>Literatur</p> | <p>Bauer, Chr.; King, G.: Hibernate in Action. Manning Pub., 2004 Bauer, A.; Günzel, H.: <i>Data-Warehouse-Systeme: Architektur, Entwicklung, Anwendung</i>, dpunkt, 2008</p> |

| | |
|--|---|
| | <p>Ganczarski, J.: <i>Data Warehouse Implementations: Critical Implementation Factors Study</i>, VDM Verlag Dr. Müller, 2009</p> <p>von Maur, E.; Winter, R.: <i>Data Warehouse Management: Das St. Galler Konzept zur ganzheitlichen Gestaltung der Informationslogistik. Metadaten, Datenqualität, Datenschutz, Datensicherheit</i>, Springer 2003</p> <p>Holten, R.: <i>Entwicklung einer Modellierungstechnik für Data Warehouse -Fachkonzepte</i>, Proc. MobIS Fachtagung, Münster, 2000</p> <p>Goeken, M.: <i>Anforderungsmanagement bei der Entwicklung von Data Warehouse Systemen – Ein sichtenspezifischer Ansatz</i>, Springer 2005</p> <p>Goeken, M.; Burmester, K.: <i>Benutzerorientierter Entwurf von unternehmensweiten Data Warehouse Systemen</i>, Springer, 2005</p> <p>Anahory, Murray: <i>Data Warehouse: Planung, Implementierung und Administration</i>, Addison Wesley, 1997</p> <p>Kempfer, H.-G.; Mehanna, W., Unger, C.: <i>Business Intelligence – Grundlagen und praktische Anwendungen</i>, Vieweg, 2. Auflage, 2006</p> <p>Manhart, K.: <i>BI-Datenmanagement (Teil 1): Datenaufbereitung durch den ETL-Prozess</i>, 2008, http://www.tecchannel.de</p> <p>Müller, R.M, Lenz, H.-J.: <i>Business Analytics</i>, Springer Vieweg 2013</p> <p>Kaiser, C.: <i>Business Intelligence 2.0</i>, Springer Gabler, 2012</p> <p>Kemper, H.-G., Baars, H., Mehanna, W.: <i>Business Intelligence - Grundlagen und praktische Anwendungen</i>, 3. Ausgabe, Springer Vieweg 2010</p> <p>Klein, A., Gräf, J.: <i>Reporting und Business Intelligence</i>, Haufe 2014</p> <p>Manhart, K.: <i>BI-Datenmanagement (Teil 2): Datensammlung und Data Warehouses</i>, 2008 , http://www.tecchannel.de</p> <p><i>OLAP-Essential</i>, http://education.oracle.com/pls/web_prod-plq-dad/show_desc.redirect?dc=D70039GC10&p_org_id=1001&lang=US</p> <p><i>Data Mining with Oracle Database 11g, Release 2</i>, Oracle White Paper September 2009, http://www.oracle.com/us/products/database/options/data-mining/039550.pdf</p> <p><i>Online Analytic Processing with Oracle Database 11g Release 2</i>, Oracle White Paper, September, 2009 http://www.oracle.com/technetwork/database/options/olap/olap-option-database-11g171752.pdf</p> <p><i>Optimizing and Protecting Storage with Oracle Database 11g, Release 2</i>, Oracle White Paper, November, 2009, http://www.oracle.com/technetwork/database/features/storage/database-11gr2-managing-storage-whi-131523.pdf</p> |
|--|---|

| | | | |
|---|---|---|---------------------|
| Modulbezeichnung | 23700 GUI-Development (Graphical User Interface-Development) | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 23700 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen GUI-Development Praktikum GUI-Development | | |
| Studiensemester | 5 | | |
| Modulverantwortliche(r) | Prof. Dr. Ute Matecki, Prof. Dr. Jörg Röhrle | | |
| Dozent(in) | Prof. Dr. Ute Matecki | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | Application-Development | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 5 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung & Übungen: | 3 SWS, Gruppengröße bis 150 | |
| | Praktikum: | 1 SWS (jeweils geblockt auf 90 min), Gruppengröße bis 20 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 45 h | 30 h |
| | Praktikum | 15 h | 60 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 12000 Programmierung 1 14500 Programmierung 2 | | |
| Modulziele / Angestrebte Lernergebnisse | Kenntnisse <ul style="list-style-type: none"> Die Studierenden kennen die unterschiedlichen Entwurfsparadigmen für Desktop-, Web- und Mobile GUIs (ergonomische Sicht). Sie kennen Schichtenmodelle und MVC-Architekturen, sowie Event-Verarbeitungsmechanismen. | | |

| | |
|--------|---|
| | <ul style="list-style-type: none"> • Sie kennen Aufbau und Funktionsweise von Widgets für RCP-Anwendungen (beispielsweise Eclipse SWT /RCP) • Sie kennen Aufbau und Funktionsweise von Widgets für mobile Anwendungen (beispielsweise Android) <p>Fertigkeiten</p> <ul style="list-style-type: none"> • Die Studierenden sind in der Lage, eigenständig GUI-Anwendungen (beispielsweise SWT/RCP) auf Basis von gegebenen Anforderungen zu entwickeln • Die Studierenden sind in der Lage, eigenständig mobile Applikationen auf Basis von gegebenen Anforderungen zu entwickeln (beispielsweise Android). <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • Sie können die Denkweise und Begrifflichkeiten in der GUI-Entwicklung selbstständig anwenden. Sie sind in der Lage, sich auch weitere Widget-Sets eigenständig anzueignen. • kennen gängige Prozessmodelle in der Softwareentwicklung und können formale Vorgehensmodelle und andere Regelwerke (z. B. StyleGuides) im Software-entwicklungsprozess adäquat an die gegebene Situation anpassen und anwenden • können geeignete Patterns in den verschiedenen Phasen der Softwareentwicklung erkennen und umsetzen <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <ul style="list-style-type: none"> • Die Studierenden haben ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um betriebliche Anwendungssysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren. • Sie können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen. • Sie sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in Bezug auf einen bestimmten Anwendungsbedarf zu verfolgen. |
| Inhalt | <p>Vorlesung & Übungen</p> <ul style="list-style-type: none"> • Arten von GUIs • Entwurfsparadigmen für GUIs (Ergonomische Sicht), StyleGuides, Unterschiede Desktop-Oberflächen, Web-Oberflächen, Mobile Anwendungen, Widgets, Widget-Sets • Weiterführung und Verallgemeinerung von GUI-Architekturen (siehe MVC-Paradigma in Modul "Programmierung 2"): Schichtenmodelle, verschiedene MVC-Umsetzungen, Thread-Aufteilung, Eventmodelle • Entwicklung von RCP-Anwendungen (beispielsweise Eclipse-SWT/RCP) |

| | |
|--|---|
| | <ul style="list-style-type: none"> • Grundlagen der GUI-Entwicklung für mobile Anwendungen (beispielsweise Android) • Internationalisierung von GUIs <p>Praktikum</p> <ul style="list-style-type: none"> • Aufgabe 1: Spezifikation und Entwicklung einer komplexen Desktop-Oberfläche (ca. 4 Wochen) • Aufgabe 2: Spezifikation und Entwicklung einer mobilen Applikation (ca. 4 Wochen) |
| Studien-/Prüfungsleistungen/ Prüfungsformen | GUI-Development: Klausur Praktikum GUI-Development: Laborarbeit (unbenotet) |
| Medienformen | Vorlesung mit Beamer, Skript in PDF-Format über Lernplattform, Praktikum in einem Labor |
| Literatur | Mobile Design Patterns Gallery: UI Patterns for Smartphone Apps, T. Neil, O'Reilly, 2014 Designing the User Interface, B. Shneiderman, Addison-Wesley, 2013 Java Native Interfaces with SWT/JFace, J. L. Guojie, Wiley & Sons, 1. edition, 2009. Professional Android 4 Application Development, Reto Meier, John Wiley and Sons, 3. edition, 2012 Eclipse 4 Application Development. L. Vogel. Lars Vogel, 2012 Rich Clients mit dem Eclipse 4.2 SDK, M. Teufel et al., entwickler.press, 2012 Eclipse RCP im Unternehmenseinsatz, S. Reichert, dpunkt, 2009 |

| | | | |
|--|--|--|---------------------|
| Modulbezeichnung | 23800 Softwarearchitektur | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 23800 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung Software-Architektur Praktikum Software-Architektur | | |
| Studiensemester | 5 | | |
| Modulverantwortliche(r) | Prof. Dr. Konrad R. Theobald, Prof'in Dr. Ute Matecki | | |
| Dozent(in) | Prof. Dr. Konrad R. Theobald, Prof'in Dr. Ute Matecki | | |
| Sprache | Deutsch (deutsches und englisches Literaturstudium erforderlich) | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | Application Development | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 5 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung & Übungen: | 3 SWS, Gruppengröße max. 150 | |
| | Praktikum: | 1 SWS, Gruppengröße max. 20 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung | 45 h | 60 h *) |
| | Praktikum | 15 h | 30 h |
| | Summe: 150h (5 * 30 Std./ECTS) | | 60 h |
| *) inklusive mündlicher Prüfung und deren Vorbereitung | | | |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 12000 Programmierung 1 14500 Programmierung 2 22300 Software Engineering | | |
| Angestrebte Lernergebnisse | Kenntnisse Die Studierenden kennen | | |

| | |
|--|--|
| | <ul style="list-style-type: none"> • die Bedeutung und Notwendigkeit der Betrachtung und Entwicklung von Software-Architekturen für komplexe Software-Produkte |
| Modulziele / Angestrebte Lernergebnisse | <ul style="list-style-type: none"> • wichtige Architekturmuster und –Stile • kennen die Aufgabe der Rolle des Software-Architekten und seines Zusammenwirkens mit anderen am Entwicklungsprozess Beteiligten <p>Fertigkeiten</p> <p>Die Studierenden sind in der Lage,</p> <ul style="list-style-type: none"> • gegebene Software-Architekturen zu lesen und zu verstehen und im Rahmen der Software-Entwicklung sinnvoll einsetzen • Software-Architekturen zu dokumentieren, und auf Qualität zu prüfen • Wiederverwendung zum Zwecke der Steigerung von Produktivität und Qualität einzusetzen, Muster einzusetzen <p>Kompetenzen</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> • Software-Architekturen in Ansätzen entwickeln • kennen gängige Prozessmodelle in der Softwareentwicklung und können formale Vorgehensmodelle und andere Regelwerke (z. B. StyleGuides) im Software-entwicklungsprozess adäquat an die gegebene Situation anpassen und anwenden • können geeignete Patterns in den verschiedenen Phasen der Software-entwicklung erkennen und umsetzen <p>Das Modul trägt zum Erreichen der folgenden Kompetenzen bei:</p> <ul style="list-style-type: none"> • sind in der Lage, übergreifende Prozesse zwischen Wirtschaftseinheiten (Unternehmen, Verwaltungseinheiten) durch Anwendungssoftware zu unterstützen • haben ein vertieftes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um betriebliche Anwendungssysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben |
| Inhalt | <p>Vorlesung:</p> <ul style="list-style-type: none"> • Sinn und Zweck von Software-Architekturen • Aufgaben von Software-Architekten • Merkmale der Architekturmodellierung |

| | |
|-----------------------------|--|
| | <ul style="list-style-type: none"> • Dokumentation von Architekturen • Modellierungs- und Semantikbeschreibungssprachen • Qualität von Software-Architekturen • Evaluation und Validierung von Architekturen • Aspekte der Wiederverwendung • Architekturmuster und Musterarchitekturen • Fallstudie <p>Praktikum:</p> <ul style="list-style-type: none"> • Entwicklung, Dokumentation und Prüfung der Architektur einer einfachen Anwendung |
| Studien-/Prüfungsleistungen | Mündliche Prüfung Dauer 20 min., benotet Laborarbeit, unbenotet |
| Medienformen | <ul style="list-style-type: none"> • Multimediale Vorlesungspräsentation • Unterlagen über Internetpräsenz • Nutzung von diversen Applikationen • Praktikum unter Nutzung von Entwicklerarbeitsplätzen |
| Literatur | <p>Andresen, A.: Komponentenbasierte Softwareentwicklung mit MDA, UML 2 und XML. Hanser, 2. Auflage, 2004, ISBN-13: 978-3446229150</p> <p>Coplien, J. O., Bjørnvig, G.: Lean Architecture: for Agile Software Development. John Wiley & Sons, 2010, ISBN-13: 978-0470684207</p> <p>Eilebrecht, K., Starke, G.: Patterns kompakt: Entwurfsmuster für effektive Software-Entwicklung. Spektrum Akademischer Verlag, 3. Auflage, 2010, ISBN-13: 978-3827425256</p> <p>Erl, T.: SOA: Design Patterns. Prentice Hall International, 2008, ISBN-13: 978-0136135166</p> <p>Erl, T.: SOA: Entwurfsprinzipien für service-orientierte Architektur. Addison-Wesley, 2008, ISBN-13: 978-3827326515</p> <p>Fowler, M. et al.: Patterns of Enterprise Application Architecture. mitp, 2003, ISBN-13: 978-3826613784</p> <p>Fowler, M. Parsons, M.: Domain Specific Languages. Addison-Wesley Longman, 2010, ISBN-13: 978-0321712943</p> <p>Hofstedt, P., Wolf, A.: Einführung in die Constraint-Programmierung. Grundlagen, Methoden, Sprachen, Anwendungen. Springer, 2007, ISBN-13: 978-3540231844</p> <p>Gamma et al.: Entwurfsmuster: Elemente wiederverwendbarer objektorientierter Software. Addison-Wesley, Neuauflage, 2010, ISBN-13: 978-3827330437</p> <p>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</p> <p>Larman, C.: UML 2 und Patterns angewendet: Objektorientierte Softwareentwicklung. mitp, 2005, ISBN-13: 978-3826614538</p> <p>Maciaszek, L.A.: Requirements Analysis and System</p> |

| | |
|--|--|
| | <p>Design. Addison-Wesley Educational Publishers Inc, 3. Auflage, 2007, ISBN-13: 978-0321440365</p> <p>Oesterreich, B.: Analyse und Design mit UML 2.3: Objektorientierte Softwareentwicklung. Oldenbourg, 2004, 9. Auflage, 2009, ISBN-13: 978-3486588552</p> <p>Posch, T. et al.: Basiswissen Softwarearchitektur: Verstehen, entwerfen, wiederverwenden. Dpunkt, 3. aktualisierte und erweiterte Auflage, 2011 Verlag, 2004, ISBN: 3898642704</p> <p>Reussner, R., Hasselbring W.: Handbuch der Software-Architektur. dpunkt Verlag, 2. Auflage, 2008, ISBN-13: 978-3898645591</p> <p>Starke, G.: Effektive Softwarearchitekturen: Ein praktischer Leitfaden. Carl Hanser Verlag, 6. überarbeitete Auflage, 2014, ISBN-13: 978-3446436145</p> <p>Starke, G., Hruschka, P.: Software-Architektur kompakt: - angemessen und zielorientiert. Spektrum Akademischer Verlag, 2. Druck, 2011, ISBN-13: 978-3827420930</p> <p>Vogel, O. et al.: Software-Architektur: Grundlagen - Konzepte – Praxis. Spektrum Akademischer Verlag, 2. Auflage, 2009, ISBN-13: 978-3827419330</p> <p>Zöller-Greer, P.: Software Architekturen: Grundlagen und Anwendungen. Composita Verlag, 3. Auflage, 2010, ISBN-13: 978-3981163933</p> <p>Zörner, S., Starke, G: Softwarearchitekturen dokumentieren und kommunizieren: Entwürfe, Entscheidungen und Lösungen nachvollziehbar und wirkungsvoll festhalten. Carl Hanser Verlag, 2012, ISBN-13: 978-3446429246</p> |
|--|--|

| | | | |
|--------------------------------------|--|---|---------------------|
| Modulbezeichnung | 23900 Big Data | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 23900 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Big Data | | |
| Studiensemester | 5 | | |
| Modulverantwortliche(r) | Prof. Dr. Thomas Eppler | | |
| Dozent(in) | Prof. Dr. Thomas Eppler | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | IT-Management | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 5 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung & Übungen: | 2 SWS, Gruppengröße bis 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 30 h | 45 h |
| | Summe 75h (2,5 * 30 Std./ECTS) | 30 h | 45 h |
| Kreditpunkte (ECTS) | 2,5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 14500 Programmierung 2 21000 Datenbanken 1 | | |
| Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden kennen</p> <ul style="list-style-type: none"> • Systeme und Techniken für die parallele Datenverarbeitung • Hadoop mit den wichtigsten Addons wie Hive • MySQL Cluster <p>Fertigkeiten</p> <p>Die Studierenden können</p> | | |

| | |
|---------------|--|
| | <ul style="list-style-type: none"> • in memory Datenbanken, • Map/Reduce/YARN-Datenbanktechnologien • verteilte Datenbankmanagementsysteme anwenden. <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind fähig logisch und abstrakt zu denken • sind fähig in gigantomanistischen Dimensionen zu denken • sind fähig kalkulatorische und technische Entscheidungen zu treffen, welches DBMS für welchen Anwendungsfall für Big Data das Richtige ist und verstehen die einzelnen DBMS zu unterscheiden. • können Unternehmensdaten extrahieren, konsolidieren und für die Auswertung in geeigneten Kennzahlensystemen bzw. für Recherche / Mustererkennung aufbereiten • sind in der Lage, digitale Spuren mithilfe forensischer Methoden und Techniken zu sichern und zu analysieren • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • haben ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um betriebliche Anwendungssysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen |
| <p>Inhalt</p> | <ul style="list-style-type: none"> • Überblick zu No-SQL-Datenbanken • Map Reduce Funktion • Aufbau des DBMS Hadoop mit <ul style="list-style-type: none"> ○ Hadoop File System ○ Map Reduce ○ YARN ○ Hive ○ Partitionierung • Verteilte Datenbanken <ul style="list-style-type: none"> ○ Vertikale/horizontale Fragmentierung ○ Fragmentierungstransparenz ○ Transaktionskontrolle • MySQL Clusters <ul style="list-style-type: none"> ○ Cluster einrichten ○ Partitionstypen |

| | |
|--|---|
| | <ul style="list-style-type: none"> ○ Verwaltung von Partitionen |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur 60 min, benotet |
| Medienformen | Vorlesung mit Beamer; Skript in PDF-Format; Implementierung konkreter Anwendungsfälle und Visualisierung mit Beamer; Übungen und Tests in einem Labor |
| Literatur | <p>Ramon Wartala: Hadoop: Zuverlässige, verteilte und skalierbare Big-Data-Anwendungen, Open Source Press</p> <p>Edward Capriolo, Dean Wampler, Jason Rutherglen: Programming Hive, O'Reilly</p> <p>Tom White. Hadoop. The definitive Guide, O' Reilly</p> <p>Uni Hildesheim: MySQL Cluster, http://www.uni-hildesheim.de/rz/DOC/mysql_refman-5.1-de.html/ndbcluster.html</p> <p>Arun C. Murthy; Vinod Kumar Vavilapalli; Doug Eadline; Joseph Niemiec; Jeff Markham: Apache Hadoop (YARN), Pearson, 2014</p> |

| | | | |
|---|--|---|---------------------|
| Modulbezeichnung | 24000 IT-Management | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 24000 | | |
| ggf. Untertitel | | | |
| Lehrveranstaltung | Vorlesung & Übungen IT-Management | | |
| Studiensemeste | 5 | | |
| Modulverantwortliche(r) | Prof. Dr. Nils Herda | | |
| Dozent(in) | Prof. Dr. Nils Herda | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | IT Management | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 5 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung und Übungen: | 4 SWS, Gruppengröße bis 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 60 h | 90 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 21100 Betriebswirtschaftslehre und Management | | |
| Modulziele / Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • kennen grundlegende Konzepte des IT-Managements. • wissen, wie die zukünftige Ausrichtung der IT-Abteilung maßgeblich beeinflusst werden kann, wie die Führung, Steuerung und Organisation der IT, die IT-Strategie, die IT-Governance, das Selbstverständnis der IT im Unternehmen und die Zusammenarbeit mit anderen Fachbereichen zu gestalten ist. | | |

| | |
|--|---|
| | <ul style="list-style-type: none"> • kennen Methoden und Verfahren zur zielgerichteten Umsetzung der IT-Planung und sind befähigt eine bereichsübergreifende Zusammenarbeit mit anderen Fachbereichen zu fördern. • kennen die Instrumente zur Steuerung des IT-Bereiches, zudem sind ihnen die wesentlichen Konzepte zur Gestaltung von Unternehmensarchitekturen bekannt und sie wissen um die Herausforderungen und Konzepte zur Integration von IT-Systemen. • kennen die Hürden bei der Umsetzung einer IT-Strategie. Sie sind vorbereitet, um auf die Komplexität und den schnellen Wandel im wirtschaftlichen Umfeld der IT reagieren zu können und begreifen die damit verbundenen Herausforderungen als Chance, einen zusätzlichen Nutzen für das Unternehmen zu generieren. • kennen den Umfang an Methoden, Techniken und Werkzeuge für die Etablierung eines unternehmensweiten IT-Sicherheitsmanagement und sind mit beispielhaften Einsatzszenarien vertraut <p>Fertigkeiten</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können den Einsatz der Informationstechnologie im Kontext der strategischen Ausrichtung des Unternehmens bewerten. • sind in der Lage, systematisch eine an den Unternehmenszielen ausgerichtete IT-Strategie zu entwickeln • können die IT als Innovationstreiber des Unternehmens positionieren. • können die Managementaspekte der IT-Sicherheit im Rahmen der Entwicklung von IT-Strategien einbinden. <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können Ausrichtung von IT-Abteilungen oder IT-Bereichen in Unternehmen analysieren und beschreiben. • können Methoden zur Entwicklung und Umsetzung von IT-Strategien anwenden und beurteilen. • wenden unterschiedliche Methoden des IT-Prozessmanagements an und beherrschen zudem gängige Modellierungsverfahren • verfügen über Kenntnisse zu IT-Projektemodellen (von klassischen bis hin zu agilen Vorgehensmethoden) und können diese geeignet anwenden • können die strategischen und rechtlichen Herausforderungen von IT-Führungskräften (IT-Governance, Risk and Compliance Management) aus Sicht des CIO und des IT-Managements erklären • können Motivation, Methodiken und Tools für das IT-Architekturmanagement analysieren und anwenden |
|--|---|

| | |
|---------------|--|
| | <ul style="list-style-type: none"> • können Vorgehensweisen im Hard- und Software-Management (ITIL, Netzwerkmanagement, Client Management u.a.) beschreiben und planen • können IT-Sicherheitsarchitekturen entwerfen und deren organisatorische sowie technische Anforderungen eindeutig spezifizieren • können die Schutzziele der IT-Sicherheit (Verfügbarkeit, Vertraulichkeit und Integrität) in Unternehmen im Kontext des IT-Sicherheitsmanagements () einordnen • können aktuelle Sicherheitsgefährdungen (Cyber- und Computerkriminalität) einschätzen und ein darauf abgestimmtes IT-Sicherheitsmanagement (u.a. Risikoanalysen, Sicherheits- und Datenschutzkontrollen) im Kontext von ISMS anwenden <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • haben praxisorientierte Kenntnisse der Wirtschaftswissenschaften und ein Grundverständnis für betriebliche Problemstellungen und der Methoden ihrer Beschreibung, Spezifikation und Beurteilung • können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess aufgabenbezogen lösen; beherrschen Methoden der Präsentation sowie Dokumentation und können diese zielgruppenorientiert einsetzen • haben einen Überblick der Gesamtheit geschäftlicher Abläufe in mittelständischen Unternehmen (KMU) bis hin zum gehobenen Mittelstand (u.a. die weltweit tätigen „Hidden Champions“) • haben einen Überblick über die wesentlichen Standards und Normen in der IT-Sicherheit (u.a. ISIS12, BSI-Grundschutz und ISO 27001) • haben ein Verständnis für den Zusammenhang zwischen IT-Sicherheit, IT-Compliance sowie dem IT-Risikomanagement entwickelt |
| <p>Inhalt</p> | <p>Der Schwerpunkt „IT-Strategie und IT-Governance“ enthält die folgenden Themenräume:</p> <ul style="list-style-type: none"> • IT-Strategieentwicklung und -umsetzung • Übersicht zu Business und IT-Alignment • Übersicht zu IT-Sourcing Strategien • Übersicht zu IT-Governance • Übersicht zu Projektportfoliomanagement <p>Der Schwerpunkt „IT-Architektur- und IT-Service-Management“ enthält die folgenden Themenräume:</p> <ul style="list-style-type: none"> • IT-Lieferantenmanagement • Übersicht zu IT-Service-Management |

| | |
|--|--|
| | <ul style="list-style-type: none"> IT Architekturmanagement bis hin zu Enterprise Architecture Management (EAM) <p>Der Schwerpunkt „Führung, Steuerung und Organisation der IT“ enthält die folgenden Themenräume:</p> <ul style="list-style-type: none"> IT-Führung IT-Controlling & -Benchmarking IT-Organisation <p>Der Schwerpunkt „IT-Sicherheit“ enthält die folgenden Themenräume:</p> <ul style="list-style-type: none"> IT-Sicherheitsmanagement IT-Risikomanagement IT-Compliance Management |
| Studien- /Prüfungsleistungen/ Prüfungsformen | Klausur (90 min): benotet |
| Medienformen | Vorlesung mit Beamer, Tafel, Skript physisch sowie digital (über Lernplattform) |
| Literatur | <p>Hofmann, J.; Schmidt, W.: Masterkurs IT-Management - Grundlagen, Umsetzung und erfolgreiche Praxis für Studenten und Praktiker. 2. Auflage, Vieweg und Teubner, 2010</p> <p>Tiemeyer, E.: Handbuch IT-Management - Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis. 4. Auflage, Hanser Verlag, 2013</p> <p>Krcmar, H.: Informationsmanagement, 5. Auflage, Springer Verlag 2009</p> <p>Resch, O.: Einführung in das IT-Management - Grundlagen, Umsetzung, Best Practice, 2. Auflage, Erich Schmidt Verlag, 2011</p> <p>Hanschke, I.: Strategisches Management der IT-Landschaft - Ein Praktischer Leitfacen für das Enterprise Architecture Management, 2. Auflage, Hanser Verlag, 2010</p> <p>Bashiri, I.; Engels, C.; Heinzelmann, M.: Informatik im Fokus - Strategic Alignment, 1. Auflage, Springer Verlag, 2010</p> <p>Kersten, H., Reuter, J., Schröder, K.-W.: „IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz“, 4. Auflage, Springer Vieweg Verlag, 2013</p> <p>Sowa, A.: „Management der Informationssicherheit: Kontrolle und Optimierung“, Springer Vieweg Verlag, 2017</p> |

| | | | |
|---|---|---|---------------------|
| Modulbezeichnung | 24100 Consulting | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 24100 | | |
| ggf. Untertitel | | | |
| Lehrveranstaltung | Vorlesung & Übungen Consulting | | |
| Studiensemester | 5 | | |
| Modulverantwortliche(r) | Prof. Dr. Nils Herda | | |
| Dozent(in) | Prof. Dr. Nils Herda | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik , Wirtschaftsinformatik | |
| | Wahlrichtung: | IT-Management | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 5 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung & Übungen: | 4 SWS, Gruppengröße bis 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 60 h | 90 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 21100 Betriebswirtschaftslehre und Management | | |
| Modulziele / Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • lernen die Fragestellungen der Unternehmensberatung auf den klassischen Themenfeldern Strategie, Geschäftsprozess-optimierung und Informationstechnologie kennen. • betrachten IT Vorhaben aus einer ganzheitlichen Sichtweise und begreifen die enge Verzahnung zwischen IT Systemen und Geschäftsprozessen. • verstehen die IT-Anforderungen unterschiedlicher Unternehmensebenen sowie die Wechselwirkungen | | |

| | |
|--|---|
| | <p>bzw. Interessenskonflikte zwischen verschiedenen Organisationseinheiten.</p> <ul style="list-style-type: none"> • lernen die Fragestellungen im Bereich der IT-Sicherheit als wichtigen Teilaspekt von Beratungsdienstleistungen kennen <p>Fertigkeiten</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können im Ergebnis Verfahren der Initiierung, Planung und des Managements von Beratungsprojekten anwenden und beurteilen. • sind auf das kommerzielle Projektgeschäft von Unternehmensberatungen in seiner Vielfalt vorbereitet. • verfügen über die Fähigkeit, Anknüpfungspunkte zu anderen Beratungsfeldern zu identifizieren und geeignete Kooperationsmodi zu entwickeln. • können ganzheitliche IT-Sicherheitskonzepte für Unternehmen maßgeschneidert entwerfen <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können die strategische Ausrichtung der IT-Organisationseinheiten in Unternehmen analysieren und beschreiben. • können Methoden zur Entwicklung und Umsetzung von IT-Strategien anwenden und beurteilen. • können das Prozessmanagement im betriebswirtschaftlichen und IT-technischen Kontext anwenden und so die Potenziale aus Sicht von Unternehmensberatungen und IT-Beratungen aufzeigen. • können methodisch aufzeigen, wie Unternehmensberatungen IT-Beratungsprojekte (auch im strategischen und betriebswirtschaftlichen Kontext) konzipieren und durchführen. • können die strategischen und rechtlichen Herausforderungen von IT-Führungskräften (IT-Governance, Risk and Compliance Management aus Sicht des CIO und des IT-Managements) erklären. • können zentrale Aspekte der IT-Sicherheit im Kontext von IT-Vorgehensmodellen und IT-Systemarchitekturen integrieren. • können Maßnahmen einleiten um die Sensibilisierung der Organisation hinsichtlich neuer IT-Risiken voranzutreiben. • Können die Anwendung des IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz im Unternehmen organisieren, koordinieren und auf Angemessenheit prüfen. <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> |
|--|---|

| | |
|--|--|
| | <ul style="list-style-type: none"> • haben praxisorientierte Kenntnisse der Wirtschaftswissenschaften und ein Grundverständnis für betriebliche Problemstellungen und der Methoden ihrer Beschreibung, Spezifikation und Beurteilung. • können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen. • können Unternehmensdaten extrahieren, konsolidieren und für die Auswertung in geeigneten Kennzahlensystemen bzw. für Recherche und Mustererkennung aufbereiten. • sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in Bezug auf einen bestimmten Anwendungsbedarf zu verfolgen. • können die IT-Sicherheit zur Prüfung der Vertraulichkeit, Verfügbarkeit sowie Integrität in die Unternehmensstruktur einbetten. • können ein unternehmensweites IT-Sicherheitskonzept entwerfen und systematisch einführen. |
| Inhalt | <p>Vorlesung & Übung</p> <p>Die Studierenden können das Consulting einordnen und sind in der Lage, den Bedarf einer Organisation in diesem Bereich zu erkennen. Ihr erworbenes Wissen befähigt sie die Bewertung IT-basierter Geschäftsmodelle vorzunehmen. Sie kennen die Einsatzpotentiale der IT im Rahmen der Prozessoptimierung und können IT-Services an die Anforderungen des Unternehmens anpassen. Die Entwicklung von Konzepten und deren Implementierung in unterschiedlichen kulturellen Arbeitsumgebungen ist Ihnen vertraut. Weiterhin sind sie sensibilisiert für das Aufkommen neuer technologischer Trends und sind in der Lage, diese adäquat zu verfolgen sowie letztlich im Unternehmen umzusetzen. Dabei ist Ihnen bewusst, dass das IT-Sicherheitsmanagement eine bedeutende Rolle spielt, um die jederzeitige Vertraulichkeit über sensible Unternehmensdaten fortlaufend zu gewährleisten.</p> |
| Studien- /Prüfungsleistungen/ Prüfungsformen | Klausur (90 min): benotet |
| Medienformen | Vorlesung mit Beamer, Tafel, Skript physisch sowie digital (über Lernplattform) |
| Literatur | Amberg, M.; Bodendorf, F.; Möslein, K.: Wertschöpfungsorientierte Wirtschaftsinformatik, o. A., Springer Verlag, 2011 Lippold, D.: Die Unternehmensberatung - Von der strategischen Konzeption zur praktischen Umsetzung, o. A., Springer Verlag, 2013 Müller, A.; Schröder, H.; von Thienen, L.: Lean IT-Management - Was die IT aus Produktionssystemen lernen kann, o. A., Gabler Verlag, 2011 |

| | |
|--|--|
| | <p>Taschner, A.: Business Cases - Ein anwendungsorientierter Leitfaden, 2. Auflage, Springer Verlag, 2008</p> <p>Fink, D.: Strategische Unternehmensberatung, 1. Auflage, Vahlen Verlag, 2009</p> <p>Kersten, H., Reuter, J., Schröder, K.-W.: „IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz“, 4. Auflage, Springer Vieweg Verlag, 2013</p> <p>Sowa, A.: „Management der Informationssicherheit: Kontrolle und Optimierung“, Springer Vieweg Verlag, 2017</p> |
|--|--|

| | | | |
|---|---|---|---------------------|
| Modulbezeichnung | 24200 E-Business | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 24200 | | |
| ggf. Untertitel | | | |
| Lehrveranstaltung | Vorlesung und Übungen E-Business | | |
| Studiensemester | 5 | | |
| Modulverantwortliche(r) | Prof. Dr. Nils Herda | | |
| Dozent(in) | Prof. Dr. Nils Herda | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | IT-Management | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 5 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung & Übungen: | 2 SWS, Gruppengröße bis 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 30h | 45h |
| | Summe: 75h (2,5 * 30 Std./ECTS) | 30h | 45h |
| Kreditpunkte (ECTS) | 2,5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | Keine | | |
| Modulziele / Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> erhalten einen intensiven Einblick in verschiedene Branchen der Internetökonomie. sind mit aktuellen Aufgabenstellungen und Entwicklungen im E-Business vertraut. wissen Umfang und Ziel des Einsatzes betrieblicher E-Business Anwendungen im Kontext der unternehmerischen Tätigkeit einzuordnen und verstehen diese systematisch einzuführen. | | |

| | |
|--|---|
| | <ul style="list-style-type: none"> • vermögen aufkommende technische und wirtschaftliche Trends einzuschätzen und entsprechende innovative Konzepte situationsabhängig in das Unternehmen einzuführen. • haben sich intensiv mit den aktuellen und zukünftigen Auswirkungen des E-Business auf die Prozesslandschaft im Unternehmen sowie die damit verbundenen Implikationen für Mitarbeiter beschäftigt. • wissen um die Arten von potenziellen IT-Angriffen, die die IT-Sicherheit im Betrieb von E-Business-Plattformen gefährden könnten <p>Fertigkeiten</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind in der Lage Geschäftsmodelle verschiedener wirtschaftlicher Akteure zu bewerten. • haben die notwendigen Fähigkeiten und Kenntnisse erworben, um relevante Technologien und Verfahren zur Abwicklung von Geschäftsaktivitäten im E-Business zu bewerten und umsetzen zu können. • können projektbezogen umfassende betriebswirtschaftliche Lösungsansätze für eine Vielfalt von Aufgabenstellungen im E-Business erarbeiten und systematisch in das Unternehmen einführen. • haben das Wissen, den Betrieb sicherer E-Business-Anwendungen und -Infrastrukturen zu gewährleisten. • können Anforderungen, die an die IT-Sicherheit von E-Business-Plattformen gestellt werden, eindeutig spezifizieren und sowohl intern wie auch gegenüber Dienstleistern kommunizieren. <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können unternehmensweite Ausrichtung von IT-Abteilungen und IT-Bereichen in Hinblick auf erfolgreiche E-Business-Aktivitäten analysieren und beschreiben (bis hin zu Multi-Channel- und Omni-Channel-Strategien) • können Methoden zur Entwicklung und Umsetzung von E-Business-Strategien anwenden und beurteilen • können IT-Sicherheitskonzepte in den Architekturentwurf von Online-Shops integrieren <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in Bezug auf einen bestimmten Anwendungsbedarf zu verfolgen. • verfügen über Kenntnisse zur Konzeption neuer Geschäftsmodelltypen, die auf innovativen Informations- |
|--|---|

| | |
|---|---|
| | <p>und Kommunikationstechnologien beruhen (E-Business, Mobile-Business bis hin zu Digitalisierung, auch Industrie 4.0).</p> <ul style="list-style-type: none"> • sind in der Lage, unternehmensübergreifende Prozesse zwischen Wirtschaftseinheiten (Unternehmen, Verwaltungseinheiten) durch Anwendungssoftware zu unterstützen. • sind in der Lage, E-Business-Anwendungen im Hinblick auf ihre IT-Sicherheit zu bewerten. • können auf Basis der aktuellen Gefährdungslage eine Einschätzung über den momentanen Status der IT-Sicherheit bei Nutzung verschiedener E-Business-Kanäle geben. |
| <p>Inhalt</p> | <p>Vorlesung</p> <ul style="list-style-type: none"> • Die Internetökonomie und damit verbundene typischen Electronic Business Architekturen • Vorgehensweisen bei der Entwicklung einer Electronic Business-Strategie • Merkmale und Eigenschaften unterschiedlicher Marktausprägungen im Electronic Business (B2B, B2C usw.) • Unterschiedlich zu verwendende Elemente des Electronic Business (Strategien, Zweck und Einsatz von E-Business), damit verbundene Geschäftsprozesse, Anwendungssysteme und Schnittstellen zu Kunden sowie zu Lieferanten. • IT-Sicherheit aus organisatorischer sowie technischer Sicht hinsichtlich der Nutzung von E-Business-Anwendungen • Sicherer Datenaustausch zwischen Beteiligten unter Nutzung von E-Business-Kanälen <p>Übungen</p> <ul style="list-style-type: none"> • in Form von Fallstudien zur Bewertung von Geschäftsmodellen. Die erarbeiteten Ergebnisse werden in Form von Präsentationen aufbereitet. |
| <p>Studien- /Prüfungsleistungen/ Prüfungsformen</p> | <p>Klausur (60 min): benotet</p> |
| <p>Medienformen</p> | <p>Vorlesung mit Beamer, Tafel, Skript physisch sowie digital (über Lernplattform)</p> |
| <p>Literatur</p> | <p>Wirtz, E.: Electronic Business, 4. Auflage, Springer Verlag, 2013</p> <p>Kollmann, T.: E-Business - Grundlagen elektronischer Geschäftsprozesse in der Net Economy, 5. Auflage, Springer Verlag, 2013</p> <p>Abts, D.; Mülder, W.: Grundkurs Wirtschaftsinformatik, 8. Auflage, Springer Verlag, 2013</p> |

| | |
|--|---|
| | <p>Turowski, K., Pousttchi, K.: Mobile Commerce – Grundlagen und Techniken, o. A., Springer Verlag, 2004</p> <p>Meier, A.; Stormer, H.: eBusiness & eCommerce: Management der digitalen Wertschöpfungskette, 3. Aufl., Springer Verlag, 2012</p> <p>Maaß, C.: E-Business Management, o. A., Lucius & Lucius Verlag, 2008</p> <p>Kersten, H., Reuter, J., Schröder, K.-W.: „IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz“, 4. Auflage, Springer Vieweg Verlag, 2013</p> <p>Sowa, A.: „Management der Informationssicherheit: Kontrolle und Optimierung“, Springer Vieweg Verlag, 2017</p> |
|--|---|

| | | | |
|---|---|---|---------------------|
| Modulbezeichnung | 24300 Digitale Forensik | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 24300 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Digitale Forensik | | |
| Studiensemester | 5 | | |
| Modulverantwortliche(r) | Prof. Holger Morgenstern | | |
| Dozent(in) | Prof. Holger Morgenstern | | |
| Sprache | Deutsch (deutsches und englisches Literaturstudium erforderlich) | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | Applied IT Security | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 5 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung & Übungen: | 4 SWS, Gruppengröße max. 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 60 h | 90 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 12500 Einführung IT Security 15000 Betriebssysteme 21200 Netzwerke | | |
| Modulziele / Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • kennen die methodische Fundierung der digitalen Forensik und ihre Einbettung in die klassische analoge Forensik • verstehen Forensische Prinzipien bei der Sicherung und Analyse digitaler Spuren | | |

| | |
|--------|---|
| | <p>Fertigkeiten</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können die forensischen Untersuchungen dokumentieren und Präsentieren, z. B. vor Gericht • sind in der Lage die gelernten Techniken in verschiedenen Teilbereichen der digitalen Forensik (z.B. Datenträgerforensik, Anwendungsforensik, Digitale Forensik Mobiler Geräte) praktisch anzuwenden <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind in der Lage, digitale Spuren mithilfe forensischer Methoden und Techniken zu sichern und zu analysieren • können Unternehmensdaten extrahieren, konsolidieren und für die Auswertung in geeigneten Kennzahlensystemen bzw. für Recherche / Mustererkennung aufbereiten <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in Bezug auf einen bestimmten Anwendungsbedarf zu verfolgen • verfügen über die zur Erfüllung von Anforderungen der Berufspraxis notwendigen persönlichen Kompetenzen: eigen-verantwortliches Handeln, Zeitmanagement, Selbstorganisation • Sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben • sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt • 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 • sind sich ihrer Verantwortung gegenüber Individuen und der Gesellschaft beim Umgang mit Sicherheitsrelevanten Informationen und Sicherheitsmethoden bewusst |
| Inhalt | <p>Vorlesung & Übungen</p> <ul style="list-style-type: none"> • Einführung in forensische Wissenschaften im Allgemeinen und die Digitale Forensik im Speziellen • Methodische Fundierung der digitalen Forensik, Einbettung in die klassische analoge Forensik |

| | |
|--|--|
| | <ul style="list-style-type: none"> • 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) |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Referat 20 min., benotet |
| Medienformen | Tafel, Teilskript, Übungsblätter, Overhead, PC mit Beamer, Intranet- und Internetzugriff |
| Literatur | <p>Dewald, A., Freiling, F.: Forensische Informatik, 1. Auflage, Books on Demand, 2011</p> <p>Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3. Auflage, Academic Press, 2011</p> <p>Carrier, B.: File Systeme, Forensic Analysis, Addison Wesley, 2005</p> <p>Geschonneck, A.: Computer-Forensik (iX Edition): Computerstraftaten erkennen, ermitteln, aufklären, dpunkt.verlag, 2014</p> <p>Hayes, D.: A Practical Guide to Computer Forensics Investigations, Pearson, 2014</p> |

| | | | |
|---|---|---|---------------------|
| Modulbezeichnung | 24400 Offensive Sicherheitsmethoden | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 24400 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Offensive Sicherheitsmethoden Praktikum Offensive Sicherheitsmethoden | | |
| Studiensemester | 5 | | |
| Modulverantwortliche(r) | Prof. Dr. Tobias Heer | | |
| Dozent(in) | Prof. Dr. Tobias Heer | | |
| Sprache | Deutsch (deutsches und englisches Literaturstudium erforderlich) | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | Applied IT Security | |
| | Wahl/Pflicht: | Pflicht | |
| | Semester: | 5 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung & Übungen: | 4 SWS, Gruppengröße max. 150 | |
| | Praktikum: | 2 SWS, Gruppengröße max. 20 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 60 h | 50 h |
| | Praktikum | 30 h | 85 h |
| | Summe: 225 h (7,5 * 30 Std./ECTS) | 90 h | 135 h |
| Kreditpunkte (ECTS) | 7,5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 12500 Einführung IT Security 15000 Betriebssysteme 21200 Netzwerke 22000 Web-basierte Anwendungen | | |
| Modulziele / Angestrebte Lernergebnisse | Kenntnisse Die Studierenden <ul style="list-style-type: none"> kennen Offensive Methoden und ihre Ziele im Kontext der IT-Sicherheit, darunter den Penetrationstest, die Angriffe auf die Vertraulichkeit, Integrität oder Verfügbarkeit von | | |

| | |
|--|--|
| | <p>Systemen, Netzwerken und Kanälen, sowie das Social Engineering</p> <ul style="list-style-type: none"> • sind sich bewusst über die rechtlichen und ethischen Rahmenbedingungen bei der Anwendung von offensiven Methoden <p>Fertigkeiten</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können aktuelle offensive Methoden anwenden, um in Systeme einzudringen • können der Zugang zu übernommenen Systemen verstetigen • können relevante Informationen aus öffentlichen Quellen ermitteln und eine Analyse der Informationsfläche eines Ziels/Unternehmens durchführen • können Schwachstellen anhand von CVSS und anderen Metriken bewerten • sind in der Lage Code auf Schwachstellen hin zu analysieren <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können methodisch und fachlich eine Sicherheitsüberprüfung durch einen Penetrationstest durchführen • Gefahren in verschiedensten Systemkomponenten durch die Kenntnis der Angriffe richtig einschätzen und vermeiden • besitzen eine ingenieurmäßige Fach- und Methodenkompetenz mit tiefgehendem Informatikwissen (im Bereich Betriebssysteme und Netzwerke, verteilte Systeme) • können Unternehmensdaten extrahieren, konsolidieren und für die Auswertung in geeigneten Kennzahlensystemen aufbereiten <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in Bezug auf einen bestimmten Anwendungsbedarf zu verfolgen • verfügen über die zur Erfüllung von Anforderungen der Berufspraxis notwendigen persönlichen Kompetenzen: eigen-verantwortliches Handeln, Zeitmanagement, Selbstorganisation • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben |
|--|--|

| | |
|--|---|
| | <ul style="list-style-type: none"> • sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt • sind in der Lage Systeme sowie Anwendungen zu analysieren, entwerfen, entwickeln und pflegen, sodass sie den heutigen Maßstäben an die Sicherheit gerecht werden • 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 • sind sich ihrer Verantwortung gegenüber Individuen und der Gesellschaft beim Umgang mit Sicherheitsrelevanten Informationen und Sicherheitsmethoden bewusst |
| Inhalt | <p>Vorlesung & Übungen</p> <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> ○ Übertragungskanälen ○ Netzwerken ○ Betriebssystemen ○ Anwendungen ○ Hardwarekomponenten ○ Web-Anwendungen ○ Funksystemen • Finden von Schwachstellen durch Fuzzing und Codeanalyse <p>Praktikum</p> <p>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</p> |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur 120min., benotet Laborarbeit, unbenotet |
| Medienformen | Tafel, Teilskript, Overhead, PC mit Beamer, Intranet- und Internetzugriff |
| Literatur | <p>Kim, P.: The Hacker Playbook 2, A practical Guide to Penetration Testing, Secure Planet LLC, 2015</p> <p>Hadnagy, C.: Social Engineering, The Art of Human Hacking, Wiley Publishing Inc., 2011</p> <p>Stuttard D.: The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Auflage 2, John Wiley & Sons, 2011</p> |

| | |
|--|--|
| | <p>Erickson, J.: Hacking, The Art of Exploitation, No Starch Press, 2008</p> <p>Messner, M.: Metasploit: Das Handbuch zum Penetration-Testing-Framework, dpunkt.Verlag, 2015</p> |
|--|--|



Semester 6

| Modulbezeichnung | 31000 Integriertes praktisches Studiensemester | | | | | | | | | | | | | | | |
|--------------------------------------|--|--------------------------|----------------|---------------------|--------------------------|------|--|---------------|--|-----|-------|--|--|------------------------------------|------|-----|
| ggf. Modulniveau | | | | | | | | | | | | | | | | |
| ggf. Kürzel | 31000 | | | | | | | | | | | | | | | |
| ggf. Untertitel | | | | | | | | | | | | | | | | |
| ggf. Lehrveranstaltungen | Ausbildung in der Praxis | | | | | | | | | | | | | | | |
| Studiensemester | 6 | | | | | | | | | | | | | | | |
| Modulverantwortliche(r) | Prof. Dr. Otto Kurz, Prof. Dr. Friedwart Reuter, Prof. Holger Morgenstern | | | | | | | | | | | | | | | |
| Dozent(in) | Betreuende Dozenten | | | | | | | | | | | | | | | |
| Sprache | Deutsch (deutsches und englisches Literaturstudium erforderlich) | | | | | | | | | | | | | | | |
| Zuordnung zum Curriculum | Studiengang: IT-Security, Technische Informatik, Wirtschaftsinformatik Wahlrichtungen: alle Wahl/Pflicht: Pflichtmodul Semester: 6 Turnus: jedes Semester | | | | | | | | | | | | | | | |
| Lehrform / SWS | Ausbildung in der Praxis: 95 Präsenztage im Betrieb | | | | | | | | | | | | | | | |
| Arbeitsaufwand | <table border="0"> <thead> <tr> <th><i>Veranstaltung/Art</i></th> <th><i>Präsenz</i></th> <th><i>Eigenstudium</i></th> </tr> </thead> <tbody> <tr> <td>Ausbildung in der Praxis</td> <td>722h</td> <td></td> </tr> <tr> <td>Praxisbericht</td> <td></td> <td>28h</td> </tr> <tr> <td colspan="3"><hr/></td> </tr> <tr> <td>Summe: 750h (25 * 30 Std./ECTS)</td> <td>722h</td> <td>28h</td> </tr> </tbody> </table> | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> | Ausbildung in der Praxis | 722h | | Praxisbericht | | 28h | <hr/> | | | Summe: 750h (25 * 30 Std./ECTS) | 722h | 28h |
| <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> | | | | | | | | | | | | | | |
| Ausbildung in der Praxis | 722h | | | | | | | | | | | | | | | |
| Praxisbericht | | 28h | | | | | | | | | | | | | | |
| <hr/> | | | | | | | | | | | | | | | | |
| Summe: 750h (25 * 30 Std./ECTS) | 722h | 28h | | | | | | | | | | | | | | |
| Kreditpunkte (ECTS) | 25 | | | | | | | | | | | | | | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | | | | | | | | | | | | | | |
| Empfohlene Voraussetzungen | Sämtliche Module der ersten vier Semester (abhängig von der durchzuführenden praktischen Tätigkeit) | | | | | | | | | | | | | | | |
| Angestrebte Lernergebnisse | Das Modul trägt zum Erreichen aller allgemeinen Studienziele des Studiengangs Wirtschaftsinformatik in vollem Umfang bei Kenntnisse Die Studierenden kennen | | | | | | | | | | | | | | | |

| | |
|-----------------------------|---|
| | <ul style="list-style-type: none"> • die Regeln des ethisch verantwortlichen Handelns im globalen Wirtschaftsraum und können ihr Handeln in Abhängigkeit von den betrieblichen Notwendigkeiten daran ausrichten <p>Fertigkeiten</p> <p>Die Studierenden sind in der Lage,</p> <ul style="list-style-type: none"> • ihre Fachkompetenz aus den ersten fünf Semestern in der Praxis anzuwenden • Methoden des Wirtschaftsinformatikers in der Praxis einzusetzen <p>Kompetenzen</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> • qualifiziert in der betrieblichen Praxis angeleitet verantwortlich arbeiten • erworbene Methodenkompetenz zum Vorteil des Betriebs einzusetzen |
| Inhalt | Die Studierenden sollen projektbezogen und fachspezifisch bei der Planung, Entwicklung und Realisierung konkreter betrieblicher Projekte aus dem Berufsfeld und Inhalt des Studiengangs mitarbeiten. Bei der weitestgehend selbständigen Bearbeitung der Aufgaben sollen die während des bisherigen Studiums gewonnenen theoretischen Kenntnisse angewendet und vertieft werden |
| Studien-/Prüfungsleistungen | Praxisbericht, unbenotet |
| Betreuung/Meilensteine | <p>Während des Praxissemesters erfolgt eine Betreuung der Studierenden durch einen vom Prüfungsausschuss festgelegten Betreuer. Vor Ort erfolgt die Betreuung durch einen qualifizierten Berater des Betriebs.</p> <p>Meilensteine</p> <ul style="list-style-type: none"> • Zwischenbericht (nach 2 Monaten), ggf. mit Coaching • Praxissemesterbericht • Zeugnis oder Tätigkeitsnachweis des Firmenberaters oder Firma |
| Literatur | <p>Czenskowsky, T. et al.: Praxissemester und Praktika im Studium. Cornelsen Lehrbuch, 2001, ISBN: 3464498077</p> <p>Mayrshofer, D.; Kröger, H. A.: Prozesskompetenz in der Projektarbeit: Ein Handbuch mit vielen Praxisbeispielen für Projektleiter, Prozessbegleiter und Berater, Windmühle, 4. Auflage, 2011, ISBN: 3937444734</p> |

| Modulbezeichnung | 31500 Berufsfertigkeit | | | | | | | | | | | | | | | | | | |
|---|---|--------------------------|----------------|---------------------|----------------------------------|-----|----|--------------------------------|-----|-----|-----------------------------------|----|----|---------------------------------|-----|-----|---|------------|------------|
| ggf. Modulniveau | | | | | | | | | | | | | | | | | | | |
| ggf. Kürzel | 31500 | | | | | | | | | | | | | | | | | | |
| ggf. Untertitel | | | | | | | | | | | | | | | | | | | |
| ggf. Lehrveranstaltungen | Vorbereitende Blockveranstaltung Nachbereitende Blockveranstaltung | | | | | | | | | | | | | | | | | | |
| Studiensemester | 6 | | | | | | | | | | | | | | | | | | |
| Modulverantwortliche(r) | Prof. Dr. Konrad R. Theobald, Prof. Dr. Otto Kurz | | | | | | | | | | | | | | | | | | |
| Dozent(in) | Prof. Dr. Konrad R. Theobald, Prof. Dr. Otto Kurz, N.N. | | | | | | | | | | | | | | | | | | |
| Sprache | Deutsch (deutsches und englisches Literaturstudium erforderlich) | | | | | | | | | | | | | | | | | | |
| Zuordnung zum Curriculum | Studiengang: IT-Security Wahlrichtungen: alle Wahl/Pflicht: Pflichtmodul Semester: 6 Turnus: jedes Semester | | | | | | | | | | | | | | | | | | |
| Lehrform / SWS | Vorbereitende Blockveranstaltung: 2 SWS, Gruppengröße Vorlesung max. 60, Projekt max. 20 Nachbereitende Blockveranstaltung: 2 SWS, Gruppengröße max. 60 | | | | | | | | | | | | | | | | | | |
| Arbeitsaufwand | <table border="1"> <thead> <tr> <th><i>Veranstaltung/Art</i></th> <th><i>Präsenz</i></th> <th><i>Eigenstudium</i></th> </tr> </thead> <tbody> <tr> <td>Vorber. Blockveranst.: Vorlesung</td> <td>15h</td> <td>5h</td> </tr> <tr> <td>Vorber. Blockveranst.: Projekt</td> <td>15h</td> <td>40h</td> </tr> <tr> <td>Nachber. Blockveranst.: Vorlesung</td> <td>5h</td> <td>5h</td> </tr> <tr> <td>Nachber. Blockveranst.: Seminar</td> <td>25h</td> <td>40h</td> </tr> <tr> <td>Summe: 150h <i>(5 * 30 Std./ECTS)</i></td> <td>60h</td> <td>90h</td> </tr> </tbody> </table> | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> | Vorber. Blockveranst.: Vorlesung | 15h | 5h | Vorber. Blockveranst.: Projekt | 15h | 40h | Nachber. Blockveranst.: Vorlesung | 5h | 5h | Nachber. Blockveranst.: Seminar | 25h | 40h | Summe: 150h <i>(5 * 30 Std./ECTS)</i> | 60h | 90h |
| <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> | | | | | | | | | | | | | | | | | |
| Vorber. Blockveranst.: Vorlesung | 15h | 5h | | | | | | | | | | | | | | | | | |
| Vorber. Blockveranst.: Projekt | 15h | 40h | | | | | | | | | | | | | | | | | |
| Nachber. Blockveranst.: Vorlesung | 5h | 5h | | | | | | | | | | | | | | | | | |
| Nachber. Blockveranst.: Seminar | 25h | 40h | | | | | | | | | | | | | | | | | |
| Summe: 150h <i>(5 * 30 Std./ECTS)</i> | 60h | 90h | | | | | | | | | | | | | | | | | |
| Kreditpunkte (ECTS) | 5 | | | | | | | | | | | | | | | | | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | | | | | | | | | | | | | | | | | |
| Empfohlene Voraussetzungen | Für die Nachbereitende Blockveranstaltung: Absolvierte Ausbildung in der Praxis | | | | | | | | | | | | | | | | | | |
| Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden kennen</p> <ul style="list-style-type: none"> • Kriterien zu einer erfolgreichen Teamarbeit | | | | | | | | | | | | | | | | | | |

| | |
|--|---|
| | <ul style="list-style-type: none"> • Methoden zur Eigenmotivation und Bewertung ihres beruflichen Leistungsvermögens • die Bedeutung ihres Verhaltens bzgl. der Selbsteinschätzung und möglicher Fremdbewertungen • die Anforderungen einer leistungsorientierten Gesellschaft • die erwarteten Charaktereigenschaften eines vorbildlichen Mitarbeiter und einer akzeptierten Führungskraft • Grundlagen der Wissenschaftsethik <p>Fertigkeiten</p> <p>Die Studierenden sind in der Lage,</p> <ul style="list-style-type: none"> • 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 <p>Kompetenzen</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> • sich mit Unternehmenszielen identifizieren • sich selbst motivieren • sich als qualifizierter Mitarbeiter in Unternehmen eingliedern • umfangreiche Formen der zweckdienlichen Kooperation zielorientiert einsetzen • mit einem hohen Maß an Toleranz erfolgsorientiert handeln • sich zur der Optimierung ihrer persönlichen Charaktereigenschaften Ziele setzen und an deren Erreichung arbeiten • sich kritisch einschätzen und & ihre Leistungen optimieren • auch in widersprüchlichen Situationen tragfähig entscheiden • ihre eigenen Leistungen bewerten und sich kritisch hinterfragen <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • haben einen Überblick der Gesamtheit geschäftlicher Abläufe in mittelständischen Unternehmen (KMU) bis hin zum gehobenen Mittelstand („Hidden Champions“) |
|--|---|

| | |
|------------------------------------|--|
| | <ul style="list-style-type: none"> • können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen • können sich und die Wirkung ihrer Person auf andere einschätzen und beweisen sich durch ihre adäquaten Mitarbeiterqualifikationen; beherrschen eine kooperative Teamarbeit in der sie Verantwortung tragen können und auch in widersprüchlichen Situationen tragfähige Entscheidungen treffen können • beherrschen selbstorganisiertes Lernen, können sich selbst motivieren, besitzen ein hohes Leistungsvermögen; kennen die Notwendigkeit der Selbstreflexion und handeln persönlich und in ihrer Arbeit kompetent |
| <p>Inhalt</p> | <p>Vorbereitende Blockveranstaltung</p> <p>Vorlesung:</p> <ul style="list-style-type: none"> • Bedeutung sozialer Kompetenz für die Berufsfertigkeit (Employability) • Wesenszüge erfolgreicher Kooperation und zielorientierter Teamarbeit • Erwartungen an die Persönlichkeit von Mitarbeitern • Methoden zur Leistungsbewertung • Moderation und Konfliktlösung • Motivationsförderung • Ethische Verantwortung des Mitarbeiters <p>Projekt:</p> <ul style="list-style-type: none"> • Durchführung eines selbstgewählten fachspezifischen gecoachten Projektes mit durchgängiger Reflexion und Evaluation in Teamarbeit unter Selbstorganisation und Projektsteuerung <p>Nachbereitende Blockveranstaltung</p> <p>Vorlesung:</p> <ul style="list-style-type: none"> • Methoden zur Komplexitätsbewältigung • Komplexes Zeit- und Projektmanagement • Methoden zur Validierung, Evaluierung und Verifikation von Projekten • Verfahren zum Wissens- und Methodentransfer • Kreativität und Innovativität <p>Seminar:</p> <ul style="list-style-type: none"> • Erarbeitung und Halten eines wissenschaftlichen Vortrags |
| <p>Studien-/Prüfungsleistungen</p> | <p>Praktische Arbeiten: benotet</p> <p>Referate: Dauer je 20 min., benotet</p> |

| | |
|--------------|---|
| Medienformen | <ul style="list-style-type: none"> • Multimediale Vorlesungspräsentation • Unterlagen über Internetpräsenz • Nutzung von diversen Applikationen • Projekt unter Nutzung von diversen Medien |
| Literatur | <p>Deutsches Institut f. Erwachsenenbildung, Deutsches Institut f. Internationale Pädagogische Forschung, Institut f. Entwicklungsplanung u. Strukturforschung: ProfilPASS - Gelernt ist gelernt: Dokumentation eigener Kompetenzen und des persönlichen Bildungswegs. Bertelsmann, 2006, ISBN-13: 978-3763935154</p> <p>Duarte, N., Heymann-Reder; D.: slide:ology: Oder die Kunst, brillante Präsentationen zu entwickeln. O'Reilly, 2009, ISBN-13: 978-3897219397</p> <p>Fischer-Epe, M., Epe, C.: Selbstcoaching:: Hintergrundwissen, Anregungen und Übungen zur persönlichen Entwicklung. Rororo, 3. Auflage, 2007, ISBN-13: 978-3499622830</p> <p>Fischer-Epe, M., Epe, C.: Stark im Beruf, erfolgreich im Leben. Persönliche Entwicklung und Selbst-Coaching. Anaconda, 2010, ISBN-13: 978-3866475076</p> <p>Haeske, U.: Pocket Business: Team- und Konfliktmanagement: Teams erfolgreich leiten - Konflikte konstruktiv lösen. Cornelsen Verlag Scriptor, 3. Auflage, 2008, ISBN-13: 978-3589234097</p> <p>Hüsgen, M.: Projektteams: Das Sechs-Ebenen-Modell zur Selbstreflexion im Team - Instrument und Einsatz. Vandenhoeck & Ruprecht, 2005, ISBN-13: 978-3525451526</p> <p>Jackman, A.: Ziele setzen, Ziele erreichen. Edition Xxl, 2008, ISBN-13: 978-3897362741</p> <p>Janson, S.: Selbstorganisation und Zeitmanagement: Mit Praxistipps und Checklisten. Redline Wirtschaftsverlag, 2007, ISBN-13: 978-3636014153</p> <p>Langmaack, B.: Soziale Kompetenz: Verhalten steuert den Erfolg. Beltz, 2004, ISBN-13: 978-3407857835</p> <p>Meier, R., Bremke, P.: Qualitätsmanagement. GABAL-Verlag, 2008, ISBN-13: 978-3897498372</p> <p>Meifert, M.T., Ulrich, D.: Strategische Personalentwicklung: Ein Programm in acht Etappen. Springer, 2. Auflage, 2010, ISBN-13: 978-3642043994</p> <p>Seiwert, L.: Noch mehr Zeit für das Wesentliche: Zeitmanagement neu entdecken. Goldmann Verlag, 2009, ISBN-13: 978-3442170593</p> <p>Thom, N., Zaugg, R.J.: Moderne Personalentwicklung: Mitarbeiterpotenziale erkennen, entwickeln und fördern. Gabler, 3. Auflage, 2008, ISBN-13: 978-3834910608</p> <p>Wedmann-Tosuner, W.: Berufsfeld Management-Assistenz. Der Weg nach oben. Fachliche und persönliche Kompetenz. Walhalla U. Praetoria, 2002, ISBN-13: 978-3802946226</p> <p>Weiß, J., Kirchner, I.: Selbstcoaching. Persönliche Power und Kompetenz gewinnen. Heyne, 2001, ISBN-13: 978-3453190474</p> |

Semester 7

| | | | |
|---|--|---|---------------------|
| Modulbezeichnung | 32000 Simulationstechnik | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 32000 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Simulationstechnik Praktikum Simulationstechnik | | |
| Studiensemester | 7 | | |
| Modulverantwortliche(r) | Prof. Dr. Otto Kurz | | |
| Dozent(in) | Prof. Dr. Otto Kurz | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | Cyber Physical Systems | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 7 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung & Übungen : | 3 SWS, Gruppengröße bis 150 | |
| | Praktikum: | 1 SWS, Gruppengröße bis 20 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 45 h | 30 h |
| | Praktikum | 15 h | 60 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 12000 Programmierung 1 14500 Programmierung 2 | | |
| Modulziele / Angestrebte Lernergebnisse | Kenntnisse Die Studierenden kennen: <ul style="list-style-type: none"> • Die grundlegende Vorgehensweise und die Parameter zur Planung der Produktionsressourcen in realen und in virtuellen Systemen. • Analyse von Prozessen für Simulationszwecke und Methoden der Prozessmodellierung. | | |

| | |
|--|---|
| | <ul style="list-style-type: none"> • Informationsmodelle der Simulation. • Grundelemente und Algorithmen zur Modellbildung der ereignisorientierten Simulation (Objekte, Methoden, Klassen, Instanzen). • Grundlagen der Statistik und Warteschlangentheorie. • Störgrößen im Produktionsablauf und deren Berücksichtigung in Simulationsmodellen. • Bewertungsverfahren für Simulationsmodelle. <p>Fertigkeiten</p> <p>Die Studierenden können:</p> <ul style="list-style-type: none"> • Betriebs- und Produktionsstrukturen analysieren und die zur Simulation erforderlichen Parameter erfassen. • Die Methoden der Modellbildung anwenden und Simulationsmodelle entwerfen, erstellen und erweiterte Algorithmen integrieren. • Simulationsmodelle optimieren nach den Kriterien: minimale Durchlaufzeit, maximale Kapazitätsauslastung, optimale Puffergrößen, maximale Flexibilität, etc... • Verfahren und Algorithmen anwenden die geeignet sind um komplexe Aufgaben in Simulationsmodelle 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 wirtschaftlichen Gesichtspunkten. <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind fähig Technisch/organisatorische Prozesse in Simulationsmodelle zu überführen und daraus Vorhersagen für die Praxis abzuleiten. • Vertiefen und festigen der Grundkenntnisse zur Optimierung von Produktionsprozessen durch Simulation. • 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 • sind in der Lage, die Planung, den Entwurf, die Implementierung und den Betrieb von Hardware/Software-Systemen wirkungsvoll zu unterstützen • sind in der Lage, den in den technischen Anwendungsbereichen der Informatik stattfindenden und sich kontinuierlich verstärkenden Einzug von Informations-technologie wirkungsvoll zu unterstützen und aktuelle Trendthemen der IT (z.B. „Internet der Dinge“, „Industrie 4.0“, „Elektro-mobilität“, „Energiewende“) in die praktische Anwendung zu überführen |
|--|---|

| | |
|--------|---|
| | <ul style="list-style-type: none"> • sind in der Lage, Kunden bei der Planung und Auswahl sowie beim Betrieb und Management komplexer und sicherer Informatiklösungen zur Optimierung von Produktions- und Arbeitsabläufen in Unternehmen zu beraten und zu unterstützen. Sie können geeignete Schulungskonzepte entwickeln und Schulungen und Unterweisungen durchführen • beherrschen wichtige Anwendungen der Technischen Informatik (Simulationstechnik Bildverarbeitung, Automobilanwendungen, Robotik, Mobile Computing / Cloud Computing) und können diese für allgemeine und spezielle Anwendungen weiterentwickeln und optimieren • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in Bezug auf einen bestimmten Anwendungsbedarf zu verfolgen • verfügen über die zur Erfüllung von Anforderungen der Berufspraxis notwendigen persönlichen Kompetenzen: eigenverantwortliches Handeln, Zeitmanagement, Selbstorganisation • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben |
| Inhalt | <p>Vorlesung & Übungen</p> <ul style="list-style-type: none"> • 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, Objekte, Klassen, Instanzen zur Prozessmodellierung. • Grundelemente, Algorithmen und Modellbildung zur objekt- und ereignisorientierten Simulation. • Grundlagen der Statistik und Warteschlangentheorie. • Störgrößenstatistik der simulierten Ressourcen und deren Berücksichtigung in Simulationsmodellen. • Modellbildungstheorie, Systemarchitekturen. • Informationsmodelle der Simulation. |

| | |
|--|--|
| | <ul style="list-style-type: none"> • Virtuelle und reale Prozessketten, Rapid Prototyping (Verfahren, Schnittstellen). • Managementkonzepte für virtuelle Entwicklungs- und Produktionsstrukturen. • Bewertung von Simulationsmodellen (technisch / wirtschaftlich). • Verteilte Simulation. • Wirtschaftlicher und technischer Nutzen der Simulation. <p>Praktikum</p> <ul style="list-style-type: none"> • Prozessanalyse, Definition von Simulationsszenarien. • Simulationsmodelle erstellen. • Simulationsmodelle erproben, modifizieren und bewerten. |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur, 90 Minuten, benotet Laborarbeit, unbenotet |
| Medienformen | Beamer + Sympodium, Tafel, Skripte und Übungsaufgaben sind als PDF-File oder Excel-Tabellen online im Intranet verfügbar. |
| Literatur | <p>Spur, G., Krause, F.-L.: Das virtuelle Produkt, Hanser Verlag, München.</p> <p>Bangsow, S.: Fertigungssimulationen mit Plant Simulation und SimTalk. Anwendung und Programmierung mit Beispielen und Lösungen, Hanser Verlag, München.</p> <p>Eley, M.: Simulation in der Logistik. Eine Einführung in die Erstellung ereignisdiskreter Modelle unter Verwendung des Werkzeuges "Plant Simulation", Springer Verlag, Berlin, New York</p> <p>Hehenberger, P.: Computerunterstützte Fertigung. Eine kompakte Einführung. 1. Aufl., Springer Verlag, Berlin, New York.</p> <p>Kramer, U.; Neculau, M.: Simulationstechnik. Hanser Verlag, München.</p> <p>Liebl, F.: Simulation. Problemorientierte Einführung, 2. Aufl., Oldenburg Verlag, München, Wien.</p> <p>Sauerbier, T.: Theorie und Praxis von Simulationssystemen. Eine Einführung für Ingenieure und Informatiker, mit Programmbeispielen und Projekten aus der Technik. Vieweg Verlag, Braunschweig, Wiesbaden.</p> |

| | | | |
|--------------------------------------|--|--|---------------------|
| Modulbezeichnung | 32100 Mobile Systeme und Cloud | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 32100 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Mobile Systeme und Cloud Praktikum Mobile Systeme und Cloud | | |
| Studiensemester | 7 | | |
| Modulverantwortliche(r) | Prof. Dr. Ute Matecki, Prof. Dr. German Nemirovski | | |
| Dozent(in) | Prof. Dr. Ute Matecki | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtungen: | Application-Development, Cyber-Physical Systems, IT-Management | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 7 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung & Übungen: | 3 SWS, Gruppengröße bis 150 | |
| | Praktikum: | 1 SWS (jeweils geblockt auf 90 min), Gruppengröße bis 20 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 45 h | 30 h |
| | Praktikum | 15 h | 60 h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 12000 Programmierung 1 14500 Programmierung 2 15000 Betriebssysteme 21200 Netzwerke | | |

| | |
|--|--|
| <p>Modulziele / Angestrebte Lernergebnisse</p> | <p>Kenntnisse</p> <ul style="list-style-type: none"> • Die Studierenden kennen die Besonderheiten mobiler Endgeräte, 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 Cloud-Services aus Anbietersicht • Sie kennen Cloud-Architekturen und Softwarelösungen für Cloud-Einsatzszenarien • Sie kennen die besonderen Anforderungen an mobile Anwendungen und Systeme, sowie die Anforderungen an Cloud-Services aus Kunden- und aus Anbietersicht <p>Fertigkeiten</p> <ul style="list-style-type: none"> • Die Studierenden sind in der Lage, eigenständig mobile Applikationen (incl. anzusprechender Sensoren) zu spezifizieren • Sie sind in der Lage, mobile Systeme nach vorgegebener/selbst erstellter Spezifikation zu entwickeln und zu testen. • Sie sind in der Lage, mobile Systeme für den Endanwender bereitzustellen (Deployment) • Die Studierenden sind in der Lage, Einsatzszenarien für Cloud Anwendungen zu verstehen und zu entwickeln (Anwendersicht). • Die Studierenden können Service-Modelle (aus Anbietersicht) entwickeln. <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind zur eigenständigen Entwicklung und Deployment mobiler Anwendungen in der Lage. Sie können eigenständig Cloud-Einsatzszenarien und Betriebsszenarien entwickeln. • kennen gängige Prozessmodelle in der Softwareentwicklung und können formale Vorgehensmodelle und andere Regelwerke (z. B. StyleGuides) im Softwareentwicklungsprozess adäquat an die gegebene Situation anpassen und anwenden • können geeignete Patterns in den verschiedenen Phasen der Softwareentwicklung erkennen und umsetzen • sind in der Lage, die Planung, den Entwurf, die Implementierung und den Betrieb von Hardware/Software-Systemen wirkungsvoll zu unterstützen • sind in der Lage, Kunden bei der Planung und Auswahl sowie beim Betrieb und Management komplexer und sicherer Informatiklösungen zur Optimierung von Produktions- und Arbeitsabläufen in Unternehmen zu beraten und zu unterstützen. Sie können geeignete Schulungskonzepte entwickeln und Schulungen und Unterweisungen durchführen |
|--|--|

| | |
|--------|---|
| | <ul style="list-style-type: none"> • 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 • sind in der Lage, praxisgerechte und kostengünstige Kundenlösungen, darunter intelligente vernetzte Geräte, für Industrie und Wirtschaft, insbesondere mit Schwerpunkten in der Informations-, Kommunikations- und Softwaretechnik, der Automobilelektronik/ –informatik zu entwickeln • beherrschen wichtige Anwendungen der Technischen Informatik (Simulationstechnik Bildverarbeitung, Automobilanwendungen, Robotik, Mobile Computing / Cloud Computing) und können diese für allgemeine und spezielle Anwendungen weiterentwickeln und optimieren • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <ul style="list-style-type: none"> • Die Studierenden haben ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um betriebliche Anwendungssysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren. • Sie können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen. • Sie sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in Bezug auf einen bestimmten Anwendungsbedarf zu verfolgen |
| Inhalt | <ul style="list-style-type: none"> • Besondere Anforderungen an mobile Anwendungen (Kundensicht und Anbietersicht) • Mobile Endgeräte, Sensoren mobiler Endgeräte • Mobiltelefonie / Drahtlose Netze und Protokolle (GSM, UMTS / IEEE 802.11, Bluetooth), Mobiles Internet, Ortsbezug • Arten Mobiler Anwendungen (Apps) • Architekturparadigmen und APIs für die Entwicklung mobiler Anwendungen (z. B. Android) • Besondere Anforderungen an Cloud-Einsatzszenarien und Betriebsszenarien (Kundensicht und Anbietersicht) • Grundlagen Virtualisierung • Service-orientierte Architekturen, Web-Services • Cloud-Arten, Service-Modelle und Cloud-Architekturen (Private Clouds, Public Clouds, SaaS,PaaS,IaaS) • Cloud-Management (Service Level Agreements, Life-Cycle, Betrieb, Kosten- und Risikomanagement) |

| | |
|--|--|
| | <ul style="list-style-type: none"> Exemplarische Betrachtung aktueller Cloud-Lösungen |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur (benotet) Laborarbeit (unbenotet) |
| Medienformen | Vorlesung mit Beamer, Skript in PDF-Format über Lernplattform, Praktikum in einem Labor |
| Literatur | Location-Based Services, J. Schiller et al., Morgan Kaufmann, 2004 Mobile Computing, K. Zeppenfeld et al., W3L GmbH, 2010 Professional Android Sensor Programming, G. Millette et al., Wrox, 2012 Cloud Computing: Web-basierte dynamische IT-Services, C. Baun et al., Springer, 2011 IaaS mit OpenStack, T. Beitter et al., d.punkt, 2014 Professional Android 4 Application Development, Reto Meier, John Wiley and Sons, 3. edition, 2012 |

| | | | |
|--------------------------------------|--|---|---------------------|
| Modulbezeichnung | 32210 Informationsvisualisierung | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 32210 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Seminar Informationsvisualisierung Projekt Informationsvisualisierung | | |
| Studiensemester | 7 | | |
| Modulverantwortliche(r) | Prof. Dr. Konrad R. Theobald | | |
| Dozent(in) | Prof. Dr. Konrad R. Theobald | | |
| Sprache | Deutsch (deutsches und englisches Literaturstudium erforderlich) | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtungen: | Application Development, IT-Security | |
| | Wahl/Pflicht: | Wahlpflichtmodul | |
| | Semester: | 7 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Seminar: | 1 SWS, Gruppengröße max. 20 Teilnehmer | |
| | Projekt: | 3 SWS, Gruppengröße max. 20 Teilnehmer | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Seminar | 15h | 30h |
| | Projekt | 45h | 60h |
| | Summe: 150h (5 * 30 Std./ECTS) | 60h | 90h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 12000 Programmierung 1 14500 Programmierung 2 15500 Algorithmen 22300 Requirements Engineering 23800 Softwarearchitektur 23410 WPF Medieninformatik | | |

| | |
|-----------------------------------|--|
| <p>Angestrebte Lernergebnisse</p> | <p>Kenntnisse</p> <p>Die Studierenden kennen</p> <ul style="list-style-type: none"> • Den aktuellen Stand der Informationsvisualisierung • die Grundlagen und Techniken der 3DModellierung • Probleme der Arbeit mit dreidimensionalen Räumen <p>Fertigkeiten</p> <p>Die Studierenden sind in der Lage,</p> <ul style="list-style-type: none"> • 3D-Anwendungen anzuwenden und zu entwickeln • Techniken der Arbeit mit dreidimensionalen Räumen in speziellen Programmumgebungen anzuwenden <p>Kompetenzen</p> <p>Die Studierenden können</p> <ul style="list-style-type: none"> • komplexe Visualisierungssysteme in Arbeitsteilung erstellen <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind dazu befähigt, betriebliche Informations- und Anwendungssysteme samt ihrer Komponenten zu analysieren und zu entwerfen. Einen besonderen Schwerpunkt stellen dabei ERP Systeme im betrieblichen Kontext dar • können Unternehmensdaten extrahieren, konsolidieren und für die Auswertung in geeigneten Kennzahlensystemen bzw. für Recherche / Mustererkennung aufbereiten • sind in der Lage, übergreifende Prozesse zwischen Wirtschaftseinheiten (Unternehmen, Verwaltungseinheiten) durch Anwendungssoftware zu unterstützen • können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben |
| <p>Inhalt</p> | <p>Seminar:</p> <ul style="list-style-type: none"> • Kennenlernen der neuesten Entwicklungen auf dem Gebiet der medialen Visualisierung komplexer Informationen • Kennenlernen und Verfügbarmachen von Entwicklungssystemen zur Programmierung medialen Visualisierungen |

| | |
|-----------------------------|---|
| | <p>Projekt:</p> <ul style="list-style-type: none"> • Umsetzen eines Teils eines Visualisierungssystems für komplexe Daten in Teamarbeit |
| Studien-/Prüfungsleistungen | (Referat + Praktische Arbeiten), benotet |
| Medienformen | <ul style="list-style-type: none"> • Unterlagen über Bibliothek und Internetpräsenz • Nutzung von diversen Applikationen • Projekt unter Nutzung von diversen Medien |
| Literatur | <p>Bassler, A.: Die Visualisierung von Daten im Controlling. Josef Eul Verlag, 2010, ISBN-13: 978-3899369397</p> <p>Bohnacker, H. et al.: Generative Gestaltung: Entwerfen. Programmieren. Visualisieren. Mit internationalen Best-Practise-Beispielen, Grundlagen, Programmcodes und Ergebnissen. Schmidt Hermann Verlag, 2009, ISBN-13: 978-3874397599</p> <p>Casey, B. F.: Processing: A Programming Handbook for Visual Designers and Artists. Mit Press, 2007, ISBN-13: 978-0262182621</p> <p>Hecht, S., Schmidl, J., Krcmar, H.: Xcelsius: Dashboarding mit SAP BusinessObjects. SAP Press, 2010, ISBN-13: 978-3836214469</p> <p>Klanten, R. et al.: Data Flow: Visualising Information in Graphic Design und Data Flow 2: Visualizing Information in Graphic Design. Die Gestalten Verlag, 2008 und 2010; ISBN-13: 978-3899552171 und ISBN-13: 978-3899552782</p> <p>Shiffman, D: Pixels, Patterns, and Processing: A Beginner's Guide to Programming Images, Animation, and Interaction. Morgan Kaufmann, 2008, ISBN-13: 978-0123736024</p> <p>Terzidis, K.: Algorithms for Visual Design Using the Processing Language. John Wiley & Sons, 2009, ISBN-13: 978-0470375488</p> <p>Tufte, E. R.: Visual Display of Quantitative Information. Graphics Press, 2. Auflag, 2001, ISBN-13: 978-0961392147</p> |

| | | | |
|---|--|---|---------------------|
| Modulbezeichnung | 32300 IT-GRC (IT-Governance, Risk & Compliance) | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | | | |
| ggf. Untertitel | | | |
| Lehrveranstaltung | Vorlesung & Übungen IT-GRC | | |
| Studiensemester | 7 | | |
| Modulverantwortliche(r) | Prof. Dr. Nils Herda | | |
| Dozent(in) | Prof. Dr. Nils Herda | | |
| Sprache | Deutsch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtungen: | Application Development, Applied IT-Security, IT Management | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Semester: | 7 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung & Übungen: | 4 SWS, Gruppengröße bis 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 60 h | 90 h |
| | Summe: 150h <i>(5 * 30 Std./ECTS)</i> | 60 h | 90 h |
| Kreditpunkte (ECTS) | 5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 21100 Betriebswirtschaftslehre und Management | | |
| Modulziele / Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • verstehen und sind in der Lage die grundlegenden Funktionen von IT-Governance, IT-Risikomanagement und IT-Compliance Management zu differenzieren. • können die einzelnen Bereiche mit Umfang und Zielsetzung in den betrieblichen Kontext einordnen und sind befähigt weitergehende Aktivitäten im Rahmen der Maturitätssteigerung dieser Funktionen zu initiieren. | | |

| | |
|--|---|
| | <ul style="list-style-type: none"> kennen die wesentlichen Frameworks im Bereich IT-Governance, IT-Risikomanagement, IT-Compliance, IT-Sicherheit und wissen diese zu kategorisieren <p>Fertigkeiten</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> sind in der Lage wesentliche Frameworks überblickhaft zu erläutern wissen Anforderungen aus den Frameworks abzuleiten. können übergreifende Handlungsempfehlungen in den Themenfeldern IT-Governance, IT-Risikomanagement und IT-Compliance Management entwickeln. <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> können Ausrichtung von IT-Abteilungen/IT-Bereichen in Unternehmen analysieren und beschreiben können Methoden zur Entwicklung und Umsetzung von IT-Strategien anwenden und beurteilen Motivation, Methodiken und Tools für das IT-Architekturmanagement analysieren und anwenden Vorgehensweisen im Hard- und Software-management (ITIL, Netzwerkmanagement, Client Management u.a.) beschreiben und planen sind in der Lage, die Sicherheitsrisiken in Unternehmen zu analysieren und darauf aufbauend Sicherheitskonzepte herzuleiten und umzusetzen können Unternehmensdaten extrahieren, konsolidieren und für die Auswertung in geeigneten Kennzahlensystemen bzw. für Recherche / Mustererkennung aufbereiten <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> können Problemstellungen erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen sind dazu befähigt, Daten und Prozessmodelle mit gängigen Modellierungsmethoden zu entwerfen, zu analysieren und Heuristiken für die Optimierung anzuwenden <p>sind in der Lage das erforderliche IT-Sicherheitsniveau für unterschiedliche Bereiche eines Unternehmens festzustellen, die einschlägigen Sicherheitsstrategien zu bestimmen, die daraus resultierenden Sicherheitsmaßnahmen einzuleiten sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in</p> |
|--|---|

| | |
|--|---|
| | Bezug auf einen bestimmten Anwendungsbedarf zu verfolgen. |
| Inhalt | <p>Vorlesung & Übungen</p> <p>Im Bereich IT-Governance werden folgende Themenbereiche schwerpunktmäßig behandelt:</p> <ul style="list-style-type: none"> • IT Governance • Schnittmenge Governance und IT-Governance • IT-Governance Frameworks • IT-Alignment • Einflussfaktoren im Bereich der IT Governance <p>Im Bereich IT-Risikomanagement werden folgende Themenbereiche schwerpunktmäßig behandelt:</p> <ul style="list-style-type: none"> • IT Risk Management • Schnittmenge Risikomanagement und IT Risikomanagement • Risikosystem IT • Risikomanagementprozesse der IT • Risikokultur und Risikovermeidung <p>Im Bereich IT-Compliance werden folgende Themenbereiche schwerpunktmäßig behandelt:</p> <ul style="list-style-type: none"> • IT Compliance Management • Compliance • nationale und internationale Compliance Regelwerke • IT Compliance und deren Diffusion im betrieblichen Kontext • Haftungsfragen der Compliance |
| Studien- /Prüfungsleistungen/ Prüfungsformen | Klausur 90min., benotet |
| Medienformen | Vorlesung mit Beamer, Tafel, Skript physisch sowie digital (über Lernplattform) |
| Literatur | <p>Knoll, M.: Praxisorientiertes IT-Risikomanagement - Konzeption, Implementierung und Überprüfung, 1. Auflage, dpunkt Verlag, 2014</p> <p>Klotz, M.: IT-Compliance: Ein Überblick, 1. Auflage, dpunkt Verlag, 2009</p> <p>Rath, M.; Sponholz, R.: IT-Compliance - Erfolgreiches Management regulatorischer Anforderungen, o. A., Erich Schmidt Verlag, 2009</p> <p>Speichert, H.: Leitfaden IT-Compliance: Rechtsfragen, Informationssicherheit und IT-Datenschutz</p> <p>Kersten, H.; Klett, G.: Der IT Security Manager: Expertenwissen für jeden IT Security Manager - Von namhaften Autoren praxisnah vermittelt, 2. Auflage, Vieweg + Teubner Verlag, 2012</p> |

| | | | |
|---|---|---|---------------------|
| Modulbezeichnung | 32400 IT-Sicherheitsmanagement | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 32400 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen IT-Sicherheitsmanagement | | |
| Studiensemester | 7 | | |
| Modulverantwortliche(r) | Prof. Holger Morgenstern | | |
| Dozent(in) | Prof. Holger Morgenstern | | |
| Sprache | Deutsch (deutsches und englisches Literaturstudium erforderlich) | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | Applied IT Security | |
| | Wahl/Pflicht: | Pflicht | |
| | Semester: | 7 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung & Übungen: | 2 SWS, Gruppengröße max. 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 30h | 45h |
| | Summe: 75h (2,5 * 30 Std./ECTS) | 30h | 45h |
| Kreditpunkte (ECTS) | 2,5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 12500 Einführung IT Security 21100 Betriebswirtschaftslehre und Management | | |
| Modulziele / Angestrebte Lernergebnisse | <p>Kenntnisse:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • kennen Grundlagen und Bedeutung des IT-Sicherheitsmanagements • kennen die Gesetzliche Anforderungen an die IT Sicherheit • kennen die IT-Sicherheitsstandards und Prozess „IT-Sicherheitsmanagement“ • verstehen IT-Sicherheitsmanagement nach BSI-Grundschutz, die Normen und die den Zertifizierungsprozess | | |

| | |
|--|--|
| | <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind in der Lage, offensive Sicherheitsmethoden im rechtlichen und moralischen Rahmen einzusetzen, um Sicherheitslücken in der Unternehmensinfrastruktur und -organisation zu identifizieren • sind in der Lage, die Sicherheitsrisiken in Unternehmen zu analysieren und darauf aufbauend Sicherheitskonzepte herzuleiten und umzusetzen <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in Bezug auf einen bestimmten Anwendungsbedarf zu verfolgen • verfügen über die zur Erfüllung von Anforderungen der Berufspraxis notwendigen persönlichen Kompetenzen: eigen-verantwortliches Handeln, Zeitmanagement, Selbstorganisation • sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt • 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 • sind sich ihrer Verantwortung gegenüber Individuen und der Gesellschaft beim Umgang mit Sicherheitsrelevanten Informationen und Sicherheitsmethoden bewusst • können wesentliche Beiträge zur Realisierung der digitalen Fabrik (Industrie 4.0) und der Automatisierung liefern. Sie konzipieren, entwickeln und implementieren dazu komplexe Informatiklösungen unter Beachtung von Wirtschaftlichkeit und Sicherheit. Sie arbeiten verantwortlich in interdisziplinären Teams |
| <p>Inhalt</p> | <p>Vorlesung & Übungen:</p> <ul style="list-style-type: none"> • Grundlagen und Bedeutung des IT-Sicherheitsmanagements • Gesetzliche Anforderungen • IT-Sicherheitsstandards • Prozess „IT-Sicherheitsmanagement“ • IT-Sicherheitsmanagement nach BSI-Grundschutz • Normen und Zertifizierung • Organisatorische Aspekte |
| <p>Studien-/Prüfungsleistungen/ Prüfungsformen</p> | <p>Klausur 60min., benotet</p> |

| | |
|--------------|--|
| Medienformen | Tafel, Teilskript, Übungsblätter, Overhead, PC mit Beamer, Intranet- und Internetzugriff |
| Literatur | <p>Hofmann, Schmidt: Masterkurs IT-Management, 2. Auflage, Springer, 2010</p> <p>Grünendahl, Steinbacher u.a.: Das IT-Gesetz: Compliance in der IT-Sicherheit, 2. Auflage, Springer, 2012</p> <p>Kersten, Reuter u.a.: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, 4. Auflage, Springer, 2013</p> <p>Müller, K.-R.: IT-Sicherheit mit System, 4. Auflage, Springer, 2011</p> <p>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</p> <p>Kersten, H.; Klett, G.: Der IT Security Manager: Expertenwissen für jeden IT Security Manager - Von namhaften Autoren praxisnah vermittelt, 2. Auflage, Springer, 2012</p> |

| | | | |
|---|--|---|---------------------|
| Modulbezeichnung | 32500 Mobile und Cloud Forensik | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | 32500 | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Vorlesung & Übungen Mobile und Cloud Forensik | | |
| Studiensemester | 7 | | |
| Modulverantwortliche(r) | Prof. Holger Morgenstern | | |
| Dozent(in) | Prof. Holger Morgenstern | | |
| Sprache | Deutsch (deutsches und englisches Literaturstudium erforderlich) | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtung: | Applied IT Security | |
| | Wahl/Pflicht: | Pflicht | |
| | Semester: | 5 | |
| | Turnus: | jedes Semester (falls Wahlrichtung zustande kommt) | |
| Lehrform / SWS | Vorlesung & Übungen: | 2 SWS, Gruppengröße max. 150 | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Vorlesung & Übungen | 30h | 45h |
| | Summe: 75h (2,5 * 30 Std./ECTS) | 30h | 45h |
| Kreditpunkte (ECTS) | 2,5 | | |
| Voraussetzungen nach Prüfungsordnung | Keine | | |
| Empfohlene Voraussetzungen | 12500 Einführung Security 15000 Betriebssysteme 21200 Netzwerke 24300 Digitale Forensik | | |
| Modulziele / Angestrebte Lernergebnisse | <p>Kenntnisse</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • kennen die speziellen Methoden der forensischen Sicherung und Analyse von mobilen Endgeräten • kennen die speziellen Methoden der digitale Forensik im Kontext des Cloudcomputings | | |

| | |
|--------|---|
| | <p>Fertigkeiten</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können die Methoden der digitalen Forensik mobiler Endgeräte und Cloud-Systeme in der Praxis anwenden <p>Kompetenzen</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • sind in der Lage, digitale Spuren mithilfe forensischer Methoden und Techniken zu sichern und zu analysieren • können Unternehmensdaten extrahieren, konsolidieren und für die Auswertung in geeigneten Kennzahlensystemen bzw. für Recherche / Mustererkennung aufbereiten <p>Das Modul trägt zum Erreichen der folgenden Lernergebnisse (Kompetenzen) bei:</p> <p>Die Studierenden</p> <ul style="list-style-type: none"> • können die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen • sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in Bezug auf einen bestimmten Anwendungsbedarf zu verfolgen • verfügen über die zur Erfüllung von Anforderungen der Berufspraxis notwendigen persönlichen Kompetenzen: eigenverantwortliches Handeln, Zeitmanagement, Selbstorganisation • sind fähig, komplexe Sachverhalte zu abstrahieren und können sie formal, logisch korrekt und präzise in der Sprache der Mathematik beschreiben • sind in der Lage Sicherheitsrisiken, sowie die Wirkungsweise von Angriffen und Schutzmaßnahmen zu verstehen und sind zur Auswahl und Anwendung von geeigneten Sicherheitstechniken befähigt • 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 • sind sich ihrer Verantwortung gegenüber Individuen und der Gesellschaft beim Umgang mit Sicherheitsrelevanten Informationen und Sicherheitsmethoden bewusst |
| Inhalt | <p>Vorlesung & Übungen</p> <ul style="list-style-type: none"> • 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 |

| | |
|--|---|
| | <ul style="list-style-type: none"> • 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 |
| Studien-/Prüfungsleistungen/ Prüfungsformen | Klausur 60min., benotet |
| Medienformen | Tafel, Teilskript, Übungsblätter, Overhead, PC mit Beamer, Intranet- und Internetzugriff |
| Literatur | <p>Bommisetty, Tamma, Mahalik: Practical Mobile Forensics, Packt Publishing, 2014</p> <p>Quick, Martini, Choo: Cloud Storage Forensics, Syngress Media, 2014</p> <p>Dewald, A., Freiling, F.: Forensische Informatik, 1. Auflage, Books on Demand, 2011</p> <p>Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3. Auflage, Academic Press, 2011</p> <p>Carrier, B.: File Systeme, Forensic Analysis, Addison Wesley, 2005</p> <p>Geschonneck, A.: Computer-Forensik (iX Edition): Computerstraftaten erkennen, ermitteln, aufklären, dpunkt.verlag, 2014</p> <p>Hayes, D.: A Practical Guide to Computer Forensics Investigations, Pearson, 2014</p> |

| | | | |
|--------------------------------------|--|---|---------------------|
| Modulbezeichnung | 51000 Bachelor-Thesis | | |
| ggf. Modulniveau | | | |
| ggf. Kürzel | | | |
| ggf. Untertitel | | | |
| ggf. Lehrveranstaltungen | Bachelor-Thesis Mündliche Bachelorprüfung | | |
| Studiensemester | 7 | | |
| Modulverantwortliche(r) | Prof. Dr. Walter Hower, Prof. Dr. Otto Kurz, Prof. Dr. K. R. Theobald | | |
| Prüfer(in) | Alle Professoren des Studiengangs Sämtliche Professoren der Fakultät; zusätzliche fachlich qualifizierte, berufserfahrene zugelassene externe Prüfer und Lehrbeauftragte | | |
| Sprache | Deutsch und/oder Englisch | | |
| Zuordnung zum Curriculum | Studiengang: | IT-Security, Technische Informatik, Wirtschaftsinformatik | |
| | Wahlrichtungen: | alle | |
| | Wahl/Pflicht: | Pflichtmodul | |
| | Turnus: | jedes Semester | |
| Lehrform / SWS | Betreute Eigenarbeit | | |
| Arbeitsaufwand | <i>Veranstaltung/Art</i> | <i>Präsenz</i> | <i>Eigenstudium</i> |
| | Bachelor-Thesis | 4 h | 356 h |
| | Mündliche Bachelorprüfung | 1 h | 89 h |
| | Summe: 450 h (15 * 30 Std./ECTS) | 5 h | 445 h |
| Kreditpunkte (ECTS) | 15 (Bachelor-Thesis: 12, Mündliche Bachelorprüfung: 3) | | |
| Voraussetzungen nach Prüfungsordnung | <p>Bachelor-Thesis: Ausgabe 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.</p> <p>Mündliche Bachelorprüfung: Frühestens 2 Monate nach Ausgabe der Bachelor-Thesis</p> | | |
| Empfohlene Voraussetzungen | Module, die in einem direkten fachlichen Zusammenhang | | |

| | |
|-----------------------------|--|
| | zur Bachelor-Thesis stehen, und die Module der ersten fünf Semester; in Absprache mit den Prüfern ggf. weiterführende Literatur |
| Angestrebte Lernergebnisse | <p>Kenntnisse: Die Studierenden kennen</p> <ul style="list-style-type: none"> • tiefgehende Kenntnisse in ihren Spezialgebieten und • umfassende Fachkenntnisse als Wirtschaftsinformatiker im Ganzen <p>Fertigkeiten: Die Studierenden sind in der Lage</p> <ul style="list-style-type: none"> • wissenschaftliche Ergebnisse strukturiert darzubieten <p>Kompetenzen: Die Studierenden können</p> <ul style="list-style-type: none"> • wissenschaftlich korrekt arbeiten • Aufgabenstellungen zielgerichtet lösen • Resultate auf wissenschaftlichem Niveau verteidigen |
| Inhalt | <p>Vorbereitung:</p> <ul style="list-style-type: none"> • Literatur-Sammlung <p>Projekt:</p> <ul style="list-style-type: none"> • Erarbeitung • Teil-Skizzen • Entwurf • Ausarbeitung <p>Prüfung:</p> <ul style="list-style-type: none"> • Vortrag • Bachelor-Arbeit und deren unmittelbares wissenschaftliches Umfeld, z. B. Quellen – sowie Inhalte der Module der ersten fünf Semester |
| Studien-/Prüfungsleistungen | Bachelor-Thesis: benotet Mündliche Bachelorprüfung: max. 45 min., davon Referat 30 min Referat und mündliche Prüfung werden gemeinsam benotet |
| Medienformen | Mündliche Präsentation (üblicherweise elektronisch gestützt) Schriftliche Ausarbeitung der Bachelor-Arbeit Ggf. weitere vorgelegte Unterlagen |
| Literatur | Bachelor-Arbeit, deren Quellen und ggf. ausgewählte Literatur in Absprache mit den Prüfern |



Zuordnung der Module zu Fächergruppen (Säulen)

In der folgenden Darstellung werden alle Module des Studiengangs IT Security den einzelnen Fächergruppen zugeordnet. Die Module *Praxissemester*, *Bachelor-Thesis* und *Mündliche Bachelorprüfung* werden gleichmäßig auf alle vier Fächergruppen verteilt, da die Zuordnung hier von der individuellen praktischer Ausrichtung abhängt.

| Informatik | | | | | | | |
|------------|---|----------|-----|-----|-------|-----------------|-----------|
| Nr. | Modul | Semester | Art | SWS | ECTS | benotet | unbenotet |
| 12000 | Programmierung 1 | 1 | PM | 6 | 7,5 | K120 | La |
| 11500 | Einführung in die Informatik | 1 | PM | 4 | 5 | K90 | |
| 14500 | Programmierung 2 | 2 | PM | 6 | 7,5 | K120 | La |
| | Web Anwendungen 1 | 2 | PM | 2 | 2,5 | Sa | |
| 15000 | Betriebssysteme | 2 | PM | 4 | 5 | K90 | La |
| 16500 | Formale Grundlagen | 2 | PM | 4 | 5 | K90 | |
| 15500 | Algorithmik | 3 | PM | 2 | 2,5 | K60 | |
| 21000 | Sichere Datenbanken | 3 | PM | 6 | 7,5 | K120 | La |
| 21200 | Netzwerke | 3 | PM | 4 | 5 | K90 | La |
| 22000 | Web Anwendungen 2 | 4 | PM | 4 | 5 | K90 | La |
| 22300 | Software Engineering | 4 | PM | 2 | 2,5 | K60 | |
| 23700 | GUI-Development | 5 | PM | 4 | 5 | K90 | La |
| 23800 | Softwarearchitektur | 5 | PM | 4 | 5 | M20 | La |
| 23600 | Datenbanken 2 | 5 | PM | 4 | 5 | M20 | |
| 31000 | Integriertes praktisches Studiensemester | 6 | PM | 0 | 25 | | Pb |
| 32500 | Mobile Systeme und Cloud | 7 | PM | 4 | 5 | K90 | La |
| 51000 | Bachelor-Thesis | 7 | PM | 0 | 15 | Ba, R30, M20 | |
| | | | | 58 | 112,5 | 17 | 10 |

| IT Security | | | | | | | |
|-------------|--|----------|-----|-----|------|---------|-----------|
| Nr. | Modul | Semester | Art | SWS | ECTS | benotet | unbenotet |
| 12500 | Einführung IT Security | 1 | PM | 4 | 5 | K90 | |
| 13000 | Einführung offensive Security- Methoden | 1 | PM | 2 | 2,5 | R15 | |
| | Digitale Logik | 1 | PM | 4 | 5 | K90 | |
| 13500 | Kryptologie 1 | 2 | PM | 4 | 5 | K90 | |
| | Kryptologie 2 | 3 | PM | 6 | 7,5 | K120 | La |
| 22600 | Netzwerk- und Systemsicherheit | 4 | PM | 4 | 5 | K90 | La |
| 22200 | Betriebssicherheit | 4 | PW | 4 | 5 | K90 | La |

| | | | | | | | |
|-------|---|---|-----|----|-----|-----------------|----|
| 22500 | Reverse Engineering | 4 | PM | 2 | 2,5 | K60 | |
| 22400 | Cyber Security | 4 | PM | 2 | 2,5 | R20 | La |
| 24300 | Digitale Forensik | 5 | PM | 4 | 5 | K90 | |
| 24400 | Offensive Sicherheitsmethoden | 5 | PM | 6 | 7,5 | K120 | La |
| 23500 | Projektstudium | 5 | PM | 6 | 7,5 | Pr | |
| 23400 | Wahlpflichtmodul 1 (WPM 1) | 5 | WPM | 4 | 5 | x | x |
| 31000 | Integriertes praktisches Studiensemester | 6 | PM | 0 | 25 | | Pb |
| 32400 | IT Sicherheitsmanagement | 7 | PM | 2 | 2,5 | K60 | |
| 32500 | Mobile und Cloud Forensik | 7 | PM | 2 | 2,5 | K60 | |
| 32200 | Wahlpflichtmodul 2 (WPM 2) | 7 | WPM | 4 | 5 | x | x |
| 51000 | Bachelor-Thesis | 7 | PM | 0 | 15 | Ba, R30, M20 | |
| | | | | 56 | 110 | 17 | 5 |

Wirtschaftsinformatik

| Nr. | Modul | Semester | Art | SWS | ECTS | benotet | unbenotet |
|-------|---|----------|-----|-----|------|-----------------|-----------|
| 22100 | Wirtschafts- und IT-Recht | 4 | PM | 4 | 5 | K90 | |
| 23900 | Big Data | 5 | PM | 2 | 2,5 | K60 | |
| 23400 | Wahlpflichtmodul 1 (WPM 1) | 5 | WPM | 4 | 5 | x | x |
| 24200 | E-Business | 5 | PM | 2 | 2,5 | K60 | |
| 31000 | Integriertes praktisches Studiensemester | 6 | PM | 0 | 25 | | Pb |
| 32200 | Wahlpflichtmodul 2 (WPM 2) | 7 | WPM | 4 | 5 | x | x |
| 32300 | IT-GRC | 7 | PM | 4 | 5 | K90 | |
| 51000 | Bachelor-Thesis | 7 | PM | 0 | 15 | Ba, R30, M20 | |
| | | | | 24 | 70 | 8 | 2 |

Technische Informatik

| Nr. | Modul | Semester | Art | SWS | ECTS | benotet | unbenotet |
|-------|---|----------|-----|-----|------|-----------------|-----------|
| 21300 | Rechnertechnik | 3 | PM | 4 | 4 | K90 | La |
| 23100 | Unternehmenskonzepte / Digitale Fabrik | 5 | PM | 4 | 5 | K90 | |
| 23200 | Verteilte Systeme (Technik) | 5 | PM | 4 | 5 | K90 | La |
| 23300 | Intelligente Lernende Systeme | 5 | PM | 4 | 5 | K90 | La |
| 23400 | Wahlpflichtmodul 1 (WPM 1) | 5 | WPM | 4 | 5 | x | x |
| 31000 | Integriertes praktisches Studiensemester | 6 | PM | 0 | 25 | | Pb |
| 32000 | Simulationstechnik | 7 | PM | 4 | 5 | K90 | La |
| 32200 | Wahlpflichtmodul 2 (WPM 2) | 7 | WPM | 4 | 5 | x | x |
| 51000 | Bachelor-Thesis | 7 | PM | 0 | 15 | Ba, R30, M20 | |
| | | | | 30 | 77,5 | 8 | 4 |

| Betriebswirtschaftslehre | | | | | | | |
|---------------------------------|--|-----------------|------------|------------|-------------|----------------|------------------|
| <i>Nr.</i> | <i>Modul</i> | <i>Semester</i> | <i>Art</i> | <i>SWS</i> | <i>ECTS</i> | <i>benotet</i> | <i>unbenotet</i> |
| 21100 | Betriebswirtschaftslehre und Management | 3 | PM | 2 | 2,5 | K60 | |
| 23000 | Projektmanagement | 5 | PM | 2 | 2,5 | Sa | |
| 24000 | IT-Management | 5 | PM | 4 | 5 | K90 | |
| 24100 | Consulting | 5 | PM | 4 | 5 | K90 | |
| 31000 | Integriertes praktisches Studiensemester | 6 | PM | 0 | 25 | | Pb |
| 51000 | Bachelor-Thesis | 7 | PM | 0 | 15 | Ba, R30, M20 | |
| | | | | 14 | 57,5 | 7 | 1 |

| Fächerübergreifende Qualifikationen | | | | | | | |
|--|--|-----------------|------------|------------|--------------|----------------|------------------|
| <i>Nr.</i> | <i>Modul</i> | <i>Semester</i> | <i>Art</i> | <i>SWS</i> | <i>ECTS</i> | <i>benotet</i> | <i>unbenotet</i> |
| 11000 | Mathematik 1 | 1 | PM | 4 | 5 | K90 | |
| 14000 | Mathematik 2 | 2 | PM | 4 | 5 | K90 | |
| 31000 | Integriertes praktisches Studiensemester | 6 | PM | 0 | 25 | | Pb |
| 31500 | Berufsfertigkeit | 6 | PM | 4 | 5 | Pr, R20 | |
| 51000 | Bachelor-Thesis | 7 | PM | 0 | 15 | Ba, R30, M20 | |
| | | | | 12 | 55 | 7 | 1 |
| Summen | | | | 194 | 482,5 | 61 | 22 |

Die Summen beziehen sich auf das **Gesamtangebot** der Module. In Abhängigkeit der individuellen Wahlrichtung ändern sich die zu erbringenden Prüfungsleistungen; die ECTS eines Gesamtstudiums belaufen sich auf **210**, die SWS auf **136** (siehe hierzu die Studien- und Prüfungsordnung des Studiengangs).

Hochschule Albstadt-Sigmaringen
IT Security
Jakobstraße 6
72458 Albstadt
Germany

+49 7571 732 9345 • win@hs-albsig.de