fiw.thws

Fakultät Informatik und Wirtschaftsinformatik

Technische Hochschule Würzburg-Schweinfurt

Modulhandbuch

Bachelor Informationssicherheit (B. Sc.)

Sommersemester 2025
Wintersemester 2025

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Inhalt

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

1. Semester

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 6810040
Algebra

Modulprofil

Prüfungsnummer
6810040

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Wintersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht

Lehrsprache
Deutsch

Organisation

Modulverantwortung
Prof. Dr. Andreas Keller

Dozierende
Prof. Dr. Andreas Keller

Verwendbarkeit	BISD
Studiensemester	1. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
Schulmathematik

Inhalte
Allgemeine Grundlagen:
- Körper der reelle Zahlen
- Prinzip der vollständigen Induktion
- Einführung in den Körper der komplexe Zahlen

Lineare Algebra:
- Vektorräume (lineare Unabhängigkeit, Basis und Dimension)
- Matrizen (Rechnen mit Matrizen, Spur und Determinante, Rang einer Matrix)
- Lineare Gleichungssysteme
- Gaußscher Algorithmus
- Lineare Abbildungen

Elementare Zahlentheorie:
- Restdarstellung ganzer Zahlen, ggT
- erweiterter Euklidischer Algorithmus
- Modulo-Rechnung
- Rechnen mit Restklassen
- Lineare Kongruenzgleichungen
- Modulare Exponentation

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
1. Die Studierenden erinnern sich an grundlegende mathematische Konzepte und Verfahren, die für die Informatik relevant sind.
2. Die Studierenden verstehen die Prinzipien der algebraischen und geometrischen Mathematik und deren Anwendung in informatischen Kontexten.
3. Die Studierenden wenden mathematische Techniken an, um Probleme aus der Informatik zu lösen und Lösungsstrategien zu entwickeln.
4. Die Studierenden analysieren mathematische Probleme und identifizieren geeignete Lösungsansätze unter Berücksichtigung verschiedener mathematischer Theorien.
5. Die Studierenden bewerten unterschiedliche Lösungsstrategien auf ihre Effizienz und Angemessenheit in der Informatik.
6. Die Studierenden erstellen mathematische Modelle, um komplexe Probleme in der Informatik zu abstrahieren und zu lösen.

Literatur
Bartholomé, Andreas; Rung, Josef; Kern, Hans: Zahlentheorie für Einsteiger. Vieweg+Teubner, Wiesbaden, 2013.
Beutelspacher, Albrecht; Zschiegner, Marc-Alexander: Diskrete Mathematik für Einsteiger. Vieweg+Teubner, Wiesbaden, 2014.
Gramlich, Günter: Lineare Algebra – Eine Einführung. Fachbuchverlag Leipzig im Carl Hanser Verlag, 2021.
Hartmann, Peter: Mathematik für Informatiker. Vieweg+Teubner, Wiesbaden, 2020.
Papula, Lothar: Mathematik für Ingenieure und Naturwissenschaftler Band 1 und 2. Vieweg+Teubner, Wiesbaden, 2018.
Pommersheim, James E.; Marks, Tim K.; Flapan, Erica L.: Number Theory: A Lively Introduction with Proofs, Applications, and Stories. John Wiley & Sons. 2010.
Schubert, Matthias: Mathematik für Informatiker. Vieweg+Teubner, Wiesbaden, 2012.
Strang, Gilbert: Lineare Algebra. Springer-Verlag, Berlin/Heidelberg/ New York, 2003.

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 5101620,6810030
Datenbanken

Modulprofil

Prüfungsnummer
5101620,6810030

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Wintersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht, Übung

Lehrsprache
Deutsch

Organisation

Modulverantwortung
Prof. Dr. Frank-Michael Schleif

Dozierende
Michael Rott

Verwendbarkeit	BIN, BISD
Studiensemester	1. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
bZv

Empfohlene Voraussetzungen
keine

Inhalte
Das Modul vermittelt die grundlegenden Konzepte und Techniken der Datenbankentwicklung. Es werden das relationale Datenmodell und die Relationen-Algebra als theoretische Grundlagen vorgestellt. Ein Schwerpunkt liegt auf der Datenbankmodellierung, insbesondere der Erstellung von Entity-Relationship-Modellen (ER-Modelle) und deren Überführung in relationale Schemata unter Berücksichtigung von Normalformen. Einführung in die Sprache SQL, einschließlich der Datenmanipulation, Datenabfrage sowie der Definition von Schemata und der Transaktionsverwaltung. In praktischen Übungen und semesterbegleitenden Projekten wird die Datenbankentwicklung und -administration geübt.

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse

- Die Studierenden können grundlegende Konzepte der Datenpersistenz und die Unterschiede zwischen persistenten und nicht-persistenten Daten erläutern.
- Die Studierenden können die zentralen Begriffe der relationalen Datenbanken, wie Relation, Primärschlüssel, Fremdschlüssel und Normalisierung, definieren.
- Die Studierenden verstehen die Relationale Algebra und können einfache Operationen darauf anwenden.
- Die Studierenden können den Zusammenhang zwischen konzeptioneller, logischer und physischer Datenmodellierung erklären und deren Bedeutung für die Datenbankentwicklung begründen.
- Die Studierenden sind in der Lage, Entity-Relationship-Modelle (ERM) für gegebene Anwendungsfälle zu erstellen und diese in relationale Schemata zu überführen.
- Die Studierenden können SQL-Abfragen zur Datenmanipulation (DML) und Schema-Definition (DDL) formulieren und ausführen.
- Die Studierenden können bestehende Datenbankschemata analysieren und hinsichtlich Redundanz, Konsistenz und Normalformen bewerten.
- Die Studierenden sind in der Lage, fachliche Informationsbedarfe zu analysieren und daraus geeignete Datenstrukturen und Abfragen abzuleiten.

Literatur

- Michael Kofler (2024). Datenbanksysteme - Das umfassende Lehrbuch (2. Auflage). Bonn: Rheinwerk Verlag GmbH
- Kemper, A., & Eickler, A. (2015). Datenbanksysteme – Eine Einführung (10. Auflage). München: De Gruyter Oldenbourg Verlag
- Elmasri, R., & Navathe, S. B. (2015). Grundlagen von Datenbanksystemen (7. Auflage). München: Pearson Studium
- Garcia-Molina, H., Ullman, J. D., & Widom, J. (2013). Database Systems: The Complete Book (2nd ed.). Upper Saddle River, NJ: Pearson
- Saake, G., Sattler, K.-U., & Heuer, A. (2011). Datenbanken – Konzepte und Sprachen (3. Auflage). München: Pearson Studium

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 5111010,6810010
Grundlagen Algorithmen und Datenstrukturen

Modulprofil

Prüfungsnummer
5111010,6810010

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Wintersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht, Übung

Lehrsprache
Deutsch

Organisation

Modulverantwortung
Prof. Dr. Frank Deinzer

Dozierende
Prof. Dr. Frank Deinzer,
Prof. Dr. Dominik Seuß

Verwendbarkeit BIN, BISD

Studiensemester 1. Semester

Art des Moduls Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
keine

Inhalte
Theoretische Themenbereiche
- Rekursion: endrekursiv/nicht endrekursiv, lineare Rekursion/ Baumrekursion
- Komplexität: O-Notation, Laufzeitkomplexität, Speicherkomplexität
- Funktionen höherer Ordnung
- (Anonyme) Lambda-Funktionen
- Abstraktionsmechanismen: Prozedurale Abstraktion, Abstraktion mit Daten
- Darstellung komplexer Datenstrukturen
- Sortieren und Suchen

Praktische Themen
- Numerische Algorithmen
- Algorithmen auf Listen
- Algorithmen auf Bäumen
- Algorithmen auf Feldern
- Algorithmen auf symbolischen Daten
- Algorithmen auf Strings
- Algorithmen auf Mengen
- Algorithmen auf Warteschlangen

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Sonstige Prüfung (soP) gemäß §§ 26, 27 APO

Dauer/Form der Prüfung
Portfolio

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Die Studierenden entwickeln zu Beginn ihrer Ausbildung ein Verständnis für Stilistik und Ästhetik der Programmierung.
Die Studierenden verstehen die grundlegenden Techniken zur algorithmischen Problemlösung.
Die Studierenden generalisieren die angemessene Anwendung wichtiger Techniken zur Beherrschung komplexer Systeme.
Die Studierenden wenden die Konzepte in den Bereichen Rekursion und Abstraktion an.
Die Stdierenden wenden Standardlösungstechniken zur Bearbeitung algorithmischer Fragestellungen an.

Literatur
Abelson, Sussman: Struktur und Interpretation von Computerprogrammen. Springer Verlag, 4. Auflage, 2014
Wagenknecht: Programmierparadigmen: Eine Einführung auf der Grundlage von Scheme. Vieweg+Teubner, 2013

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 6810050
Grundlagen der Informationssicherheit

Modulprofil

Prüfungsnummer
6810050

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Wintersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht

Lehrsprache
Deutsch

Organisation

Modulverantwortung
Prof. Dr.-Ing. Sebastian Biedermann

Dozierende
Prof. Dr.-Ing. Sebastian Biedermann

Verwendbarkeit	BISD
Studiensemester	1. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
keine

Inhalte
In diesem Modul werden Themen, die für weiterführende Module im Studiengang Informationssicherheit grundlegend sind, in der notwendigen technischen Tiefe erläutert.
Grundlagen von Betriebssystemen, Anwendungen, Computernetzwerken und der Programmierung werden stets mit Fokus auf Fragestellungen der Informationssicherheit vermittelt.
Verschiedene Typen von Angreifenden, deren Motivation und deren Geschäftsmodelle werden beispielhaft an bekannten Szenarien aus der Vergangenheit erörtert.
Des Weiteren werden die verschiedenen Berufsbilder, die damit verbundenen Aufgaben und mögliche Karriereoptionen im Bereich Informationssicherheit vorgestellt.

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Studierende...

- verstehen die grundlegenden Schutzziele der Informationssicherheit
- kennen populäre Strategien von digitalen Angriffen, die dahinterstehenden Motivationen und/oder Geschäftsmodelle
- verstehen die Funktionsweisen von Betriebssystenem und deren Sicherheitsmechanismen und Sicherheitsprobleme
- verstehen den grundlegenden Ablauf von Programmen bzw. Prozessen und damit verbundenen sicherheitsrelevanten Interaktionen
- kennen die Grundlagen digitaler Kommunikation, von Computernetzen und dem Internet
- kennen verschiedene Berufsbilder und die damit verbundenen Aufgaben im Bereich der Informationssicherheit
- können in einer Skriptsprache einfache Programme schreiben

Literatur
Jason Andress, Foundations of Information Security, 2019
Andrew S. Tanenbaum, Moderne Betriebssysteme, 4. Auflage, 2016
Andrew S. Tanenbaum, Computernetzwerke, 5. Aktualisierte Auflage, 2019
Justin Seitz & Tim Arnold, Black Hat Python, 2. Auflage, 2021

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 5000130,5100130,6810020 Programmieren I

Modulprofil

Prüfungsnummer
5000130,5100130,6810020

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Semester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht, Übung

Lehrsprache
Deutsch

Organisation

Modulverantwortung
Prof. Dr. Steffen Heinzl

Dozierende
Prof. Dr. Steffen Heinzl, Christine Zilker

Verwendbarkeit	BIN, BISD, BWI
Studiensemester	1. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
bZv

Empfohlene Voraussetzungen
keine

Inhalte
Im Modul Programmieren I geht es darum, die prozedurale Programmierung sowie erste Teile der objektorientierten Programmierung in der Programmiersprache Java zu erlernen. Die Fähigkeit, programmieren zu können und damit selbstständig kleinere Probleme in unterschiedlichen Bereichen lösen zu können, ist eine der grundlegenden Kompetenzen, die von einem (Wirtschafts-)Informatiker erwartet wird.

Der Kurs besteht aus 13 Lektionen, die aus Lernvideos, den dazugehörigen Übungen, den Power-Point-Folien zu den Videos und zum Stoff passenden Quizzen bestehen.

Die Lernvideos sind so strukturiert, dass die Studierenden nach und nach die verschiedenen Sprachkonstrukte und grundlegende Konzepte der Programmierung kennenlernen. Der begleitende Seminaristische Unterricht dient dem Stellen von Fragen und der Vertiefung des Stoffs.

Die Übungen sind der mit Abstand wichtigste Bestandteil des Kurses. Durch das eigenständige Lösen von Problemstellungen erlernen die Studierenden die Programmierung. Die Übungstermine helfen, indem Studierenden dort vom Dozenten Denkanstöße gegeben werden, wenn ein Studierender bei Aufgaben nicht weiterkommt, und die Qualität von Lösungen besprochen und verbessert werden. Die Übungen gehören in der Regel zu den vorherigen Lernvideos und greifen deren Inhalte auf.

Zu jeder Lektion gibt es ein Quiz, das durch einfache Fragen den Studierenden eine Überprüfungsmöglichkeit gibt, ob sie den behandelten Stoff wissen bzw. verstehen.

Inhalte:
- Einführung/Erstes Programm (Hallo Welt)
- Elementare Sprachkonstrukte (Ausdrücke, primitive Variablen, Zuweisungen)
- Essenzielle (Steuer-)Anweisungen (Bedingte Anweisungen, Verzweigungen, kopf- und fußgesteuerte Schleifen)
- Methoden, Rekursion, Arrays, Komplexe Datentypen
- Objektorientierung (Einführung), Klassen, Objekte, (Instanz-)Methoden, Sichtbarkeit

- Mehrdimensionale Arrays, Verhalten von Referenztypen, String-Methoden, Garbage Collector
- Datenstrukturen (einfach und doppelt verkettete Listen, Binärbäume, Traversieren von Bäumen)
- Packages, implizite Vererbung, Relationen am Beispiel von equals
- DRY-Prinzip, Tell, don't ask-Prinzip
- fakultativ: Bitweise Operatoren

- Eingesetzte IDE: Eclipse

Dieses Modul ist die Grundlage für Programmieren 2 und das Programmierprojekt. Ferner erleichtern Inhalte und erworbene Kompetenzen dieses Moduls das Modul Programmieren 3 deutlich und sind nützlich für

- Mathematische SW in der Informatik
- Algorithmen und Datenstrukturen 2
- Betriebssysteme
- Grundlagen Verteilte Systeme
- Datenmanagement & Data Science

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Nach dem erfolgreichen Abschluss des Moduls sind die Studierenden in der Lage

- prozedurale Programmierung sowie einführend auch Grundzüge der objektorientierten Programmierung anzuwenden
- eigenständig eine Lösungsstrategie zum Schreiben kleiner prozeduraler und objektorientierter Java-Programme nach einer vorgegebenen Entwurfsidee umzusetzen
- einfache mathematische und technische Problemstellungen zu verstehen und eine Lösung zu implementieren
- Teilprobleme durch geeignete Mittel zu generalisieren

Literatur
Heinisch, Cornelia; Müller-Hofmann, Frank; Goll, Joachim: Java als erste Programmiersprache; Vom Einsteiger zum Profi; Springer Vieweg, 2023
Christian Ullenboom: Java ist auch eine Insel, 17., aktualisierte und überarbeitete Auflage, Rheinwerk Computing, 2023
Reinhard Schiedermeier: Programmieren mit Java, Pearson Studium - IT, 2010

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: unbekannt
Programmieren in Python

Modulprofil

Prüfungsnummer
unbekannt

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Wintersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht, Übung

Lehrsprache
Deutsch

Organisation

Modulverantwortung
Prof. Dr. Tristan Wimmer

Dozierende
Prof. Dr. Tristan Wimmer, Christine Zilker

Verwendbarkeit	BISD
Studiensemester	1. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
keine

Inhalte
Dieses Modul zielt darauf ab, Studierenden die Grundlagen der Programmierung mithilfe der Programmiersprache Python beizubringen. Es stellt die Grundkonzepte von Programmiersprachen und Programmierparadigmen vor und schafft die Basis für weitere Module im Studiengang Software-Engineering.
Folgende Themen werden behandelt:

- Elementarer Datentypen, Datenstrukturen und Operatoren
- Kontrollstrukturen: Schleifen und bedingte Anweisungen
- Programmieren mit Funktionen
- Einführung in die objektorientierte Programmierung
- Einführung in das Konzept der Vererbung
- Einführung in das Exception Handling

Neben diesen Themen werden in diesem Modul die geeigneten Strukturierungsmöglichkeiten von Code, sowie Dokumentationsmöglichkeiten für einen sauberen und gut lesbaren Programmierstil, aufgezeigt. Desweiteren wird den Studierenden gezeigt, wie sie Problemen am besten begegnen und lösen.

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Nach erfolgreicher Absolvierung des Moduls sind Studierende in der Lage die grundlegenden Datentypen, Datenstrukturen und Operatoren zu identifizieren und zu benennen sowie diese in der Programmiersprache Python anzuwenden.

- Die Studierende sind in der Lage, zu erläutern, wie Kontrollstrukturen wie Schleifen und bedingte Anweisungen den Ablauf von Programmen steuern und wie diese in Python implementiert werden.
- Nach erfolgreicher Absolvierung des Moduls sind Studierende in der Lage, einfache Python-Programme zu schreiben, die Funktionen und Parameterübergaben nutzen, um spezifische Aufgaben zu lösen, wobei das Prinzip des Divide & Conquer angewendet wird.
- Die Studierende sind in der Lage, die objektorientierte Programmierung anzuwenden, um durch Kapselung die Struktur und Wartbarkeit eines Programms zu verbessern.
- Nach erfolgreicher Absolvierung des Moduls sind Studierende in der Lage, für eine spezifische Anforderung ein objektorientiertes Programm in Python zu entwerfen und zu implementieren, indem die grundlegenden Prinzipien der Vererbung genutzt werden.
- Nach erfolgreicher Absolvierung des Moduls sind Studierende in der Lage, Exception Handling für fehlerhafte Eingaben und Datentypinkompatibilitäten anzuwenden.

Literatur
Häberlein, Tobias. Programmieren Mit Python: Eine Einführung in Die Prozedurale, Objektorientierte Und Funktionale Programmierung. 1st ed. 2024. Berlin, Heidelberg: Springer Berlin Heidelberg, 2024. https://doi.org/10.1007/978-3-662-68678-2.

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 6810060
Social Engineering and Security Awareness

Modulprofil

Prüfungsnummer
6810060

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Wintersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht

Lehrsprache
Englisch

Organisation

Modulverantwortung
Prof. Dr. Kristin Weber

Dozierende
Prof. Dr. Kristin Weber,
Andreas Schütz

Verwendbarkeit	BISD
Studiensemester	1. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
keine

Inhalte
The module Social Engineering and Security Awareness focuses on the human factor of information security. People make a decisive contribution to information security in companies with their behaviour - they are an important security factor. Due to this influence, they are increasingly targeted by cyber criminals. The module primarily looks at these two aspects - security factor and victim - of the human factor in information security.

Information security awareness describes the sensitisation of employees for information security (security factor). The module contains the following contents on awareness:
- Concept and models, psychological understanding of awareness
- Practical examples of awareness measures
- Promoting and measuring awareness

Social engineering is the targeted manipulation of people in order to seduce them into unintentional actions (victims). The following contents, among others, are dealt with in social engineering:
- Basics and forms
- Psychological tricks
- Phishing and phishing simulations

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Englisch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Students see people as a solution and not as a problem for information security.
They explain the role of the human factor in information security using examples.
The students know and identify the principles of social engineering and can explain them using examples.
They name different forms of phishing and can discuss the advantages and disadvantages of phishing simulations.
They understand what information security awareness means and know methods to enhance the different aspects of awareness.
Students can create awareness measures in a targeted and individualised way.

Literatur
Beißel, S.: Security Awareness, De Gruyter, 2019.
Cialdini, R.: Influence – The Psychology of Persuasion, Collins Business, 2007.
Hadnagy, C. (with Schulman, S.): Human Hacking – Win Friends, Influence People, and Leave Them Better off for Having Met You, Harper Business, 2021.
Helisch, M.; Pokoyski, D. (Hrsg.): Security Awareness – Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung, Vieweg+Teubner, 2010.
Schroeder, J.: Advanced Persistent Training, Apress, 2017.
Verplanken, B. (Ed.): The Psychology of Habit – Theory, Mechanisms, Change, and Context, Springer, 2018.
Weber, K.: Mensch und Informationssicherheit, Hanser, 2024.
Weber, K.; Schütz, A.; Fertig, T.: Grundlagen und Anwendung von Information Security Awareness, SpringerVieweg, 2019.
Take Aware Sec&Life Magazin, https://www.take-aware-events.com/news-post/magazinesecandlife

2. Semester

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 9999999
Allgemeinwissenschaftliches Wahlpflichtmodul

Modulprofil

Prüfungsnummer
9999999

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Semester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminar

Lehrsprache
Deutsch/Englisch

Organisation

Modulverantwortung
Prof. Dr. Jochen Seufert

Dozierende
Beate Wassermann

Verwendbarkeit	BEC, BDGD, BISD
Studiensemester	2. Semester
Art des Moduls	AWPM

Verpflichtende Voraussetzungen gemäß SPO
i. d. R. keine; Ausnahmen werden durch die Fakultät Angewandte Natur- und Geisteswissenschaften festgelegt und bekanntgegeben.

Empfohlene Voraussetzungen
keine

Inhalte
Auswahl von zwei Allgemeinwissenschaftlichen Wahlpflichtfächern (AWPF) (2 x 2 SWS) bzw. einem AWPF (1 x 4 SWS) aus dem Fächerangebot der Fakultät Angewandte Natur- und Geisteswissenschaften (FANG).

Fächerangebot der FANG aus den Bereichen
- Sprachen
- Kulturwissenschaften
- Naturwissenschaften und Technik
- Politik, Recht und Wirtschaft
- Pädagogik, Psychologie und Sozialwissenschaften
- Soft Skills
- Kreativität und Kunst.

Ausgeschlossen aus dem Angebotskatalog der FANG sind Veranstaltungen, deren Inhalte bereits Bestandteile oder unmittelbar fachlich verwandt mit Teilen anderer Module des Studiengangs sind. Die entsprechenden Veranstaltungen sind im Fächerkatalog der FANG mit einem Sperrvermerk versehen.
Die Inhalte der einzelnen AWPFs sind auf der fakultätseigenen Homepage der FANG veröffentlicht.

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch/Englisch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Die fachspezifischen Lernziele sind abhängig von den jeweils ausgewählten AWPF. Die Studierenden

- erwerben zudem Wissen und Kompetenzen, die nicht fachspezifisch sind, aber für das angestrebte Berufsziel bedeutsam sein können wie beispielsweise spezielle Kenntnisse bei Fremdsprachen, in naturwissenschaftlichen oder auch in sozialwissenschaftlichen Gebieten
- analysieren unterschiedlichste Fragestellungen
- ordnen das fachspezifische Wissen in einen interdisziplinären Zusammenhang ein
- übertragen das Gelernte auf die aktuelle Ausbildung
- haben ihre Schlüsselkompetenzen und ggf. Fremdsprachenkompetenzen erweitert, wodurch die Persönlichkeitsbildung unterstützt wird, auch in interkultureller Hinsicht
- sind sich ihrer Verantwortung in persönlicher, gesellschaftlicher und ethischer Hinsicht bewusst.

Literatur
je nach gewählten AWPFs

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 6810100
Grundlagen der Kryptographie

Modulprofil

Prüfungsnummer
6810100

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Sommersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht, Übung

Lehrsprache
Deutsch

Organisation

Modulverantwortung
Prof. Dr. Andreas Keller

Dozierende
Prof. Dr. Andreas Keller

Verwendbarkeit	BISD
Studiensemester	2. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
Modul „Algebra“

Inhalte
- Mathematische Grundlagen
- Blockchiffren
- DES und AES
- Das RSA-Verfahren
- Kryptographische Hashfunktion
- Diskrete Logarithmen und das ElGamal-Verfahren

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Die Studierenden können nach Abschluss des Moduls:

- mathematische Konzepte der Zahlentheorie und linearen Algebra benennen, die für kryptographische Verfahren relevant sind.
- grundlegende kryptographische Verfahren wie symmetrische und asymmetrische Verschlüsselung beschreiben und voneinander unterscheiden.
- die Funktionsweise ausgewählter kryptographischer Algorithmen (z. B. RSA, Diffie-Hellman, AES) anhand mathematischer Grundlagen erklären.
- die Sicherheit kryptographischer Verfahren unter Verwendung mathematischer Kriterien (z. B. Primfaktorzerlegung, diskreter Logarithmus) analysieren.
- die Anwendbarkeit kryptographischer Verfahren in Bezug auf Schlüssellängen, Rechenaufwand und bekannte Angriffsszenarien kritisch bewerten.
- Grenzen kryptographischer Verfahren erkennen und erläutern, insbesondere im Hinblick auf theoretische und praktische Angriffe.
- kryptographische Aufgabenstellungen selbstständig und strukturiert bearbeiten.
- durch logisches Denken geeignete Lösungswege für kryptographische Probleme entwickeln und mathematisch fundiert begründen.
- die Bedeutung mathematischer Strukturen für die Sicherheit von Verschlüsselungsverfahren reflektieren.

Literatur
Beutelspacher, Wolfenstetter: Kryptografie in Theorie und Praxis, Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH, Wiesbaden 2010
Delf, Knebl: Introduction to Cryptographie, Springer Berlin, Heidelberg, 2016
Ertel: Angewandte Kryptographie, Hanser Verlag, 2018

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 6810120
ISM-Standards and Processes

Modulprofil

Prüfungsnummer
6810120

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Sommersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht

Lehrsprache
Englisch

Organisation

Modulverantwortung
Prof. Dr. Kristin Weber

Dozierende
Prof. Dr. Kristin Weber,
Prof. Dr.-Ing. Tobias Fertig

Verwendbarkeit	BISD
Studiensemester	2. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
Social Engineering and Security Awareness

Inhalte
The module Information Security Management (ISM) Standards and Processes deals with the holistic design of information security management in companies and organisations. Information security does not only mean implementing technical measures to protect the IT infrastructure. Rather, organisational, technical, physical and personnel security measures must be coordinated with each other and with the objectives of the organisation. Effective security concepts are developed, implemented, audited, and continuously improved on the basis of established frameworks, taking into account effectiveness, usability and cost efficiency.

Against this background, the module ISM Standards & Processes covers, among others, the following topics:

- Structure and content of information security management (ISM) standards and frameworks (e.g., ISO27001, BSI IT-Grundschutz, CISIS12)
- Creation of holistic information security concepts
- Organisational security measures, e.g., guidelines for information security, classification concept for information
- Metrics and maturity models for information security
- Incident response and business continuity management
- Audits of security concepts and measures

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Englisch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Students know the content and structure of ISMS standards and frameworks and select these depending on the situation.
Students create organisational security measures such as information security guidelines.
Students adapt processes such as incident response and business continuity management to organisation-specific requirements.
Students understand the relationship between effectiveness, efficiency, and usability for the selection and implementation of information security measures.
Students know concepts for the evaluation, auditing, and continuous improvement of ISMS.

Literatur
Harich, T.: IT-Sicherheitsmanagement – Praxiswissen für IT Security Manager, 2nd Ed., mitp, 2018
Harkins, M.: Managing Risk and Information Security – Protect to Enable, 2nd Ed., Apress, 2016
Kersten, H. et al.: IT-Sicherheitsmanagement nach der neuen ISO 27001 – ISMS, Risiken, Kennziffern, Controls, 2. Aufl., Springer Vieweg, Wiesbaden, 2020
Lang, M.; Löhr, H: IT-Sicherheit – Technologien und Best Practices für die Umsetzung in Unternehmen, HANSER, 2022
Sowa, A.: Management der Informationssicherheit – Kontrolle und Optimierung, Springer Vieweg, Wiesbaden, 2017
Weber, K.: Mensch und Informationssicherheit, Hanser, 2024.
Whitman, M.; Mattord, H.: Management of Information Security, Cengage Learning, 6. Aufl., 2018

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 5111120,6810070
Internetkommunikation

Modulprofil

Prüfungsnummer
5111120,6810070

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Sommersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht

Lehrsprache
Deutsch

Organisation

Modulverantwortung
Prof. Dr. Christian Bachmeir

Dozierende
Prof. Dr. Christian Bachmeir

Verwendbarkeit	BIN, BISD
Studiensemester	2. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
keine

Inhalte
Grobgliederung:
1) Einführung Kommunikationsnetze
2) Theoretische Grundlagen Kommunikationstechnik
3) Praktische Grundlagen Internet-Kommunikation
4) Einführung in IT-Security
5) Grundlagen der Kryptografie

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
1. Die Studierenden erinnern sich an grundlegende Konzepte der Kommunikationssysteme im Internet und deren technische Grundlagen.
2. Die Studierenden verstehen die Funktionsweisen der drahtlosen Kommunikationstechnik und deren Auswirkungen auf die Datenübertragung.
3. Die Studierenden wenden moderne kryptografische Verfahren an, um die Sicherheit der Internet-Kommunikation zu gewährleisten.
4. Die Studierenden analysieren die Leistungen, Möglichkeiten und Einschränkungen von Kommunikationssystemen im Internet, um fundierte Entscheidungen bei der Entwicklung verteilten Systeme zu treffen.
5. Die Studierenden verstehen und bewerten die Notwendigkeit kryptografischer Verfahren in unterschiedlichen Anwendungsszenarien des Betriebsalltags.
6. Die Studierenden erstellen Konzepte zur Implementierung von Sicherheitsmechanismen in Internet-Kommunikationssystemen basierend auf erlernten kryptografischen Techniken.

Literatur
Patrick Schnabel, Kommunikationstechnik-Fibel, Kindle eBooks
Kurose, Ross: Computernetzwerke, Der Top-Down-Ansatz, Verlag: Pearson Studium; Auflage: 6., aktualisierte Auflage, 2019
Tanenbaum, Wetherall: Computernetzwerke, Verlag: Pearson Studium; Auflage: 5., aktualisierte Auflage, 2013
Schmeh: Kryptografie: Verfahren - Protokolle - Infrastrukturen (iX-Edition) Verlag: dpunkt.verlag GmbH; Auflage: 5., aktualisierte Auflage, 2013

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 6810110
Penetration Testing

Modulprofil

Prüfungsnummer
6810110

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Sommersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht

Lehrsprache
Deutsch/Englisch

Organisation

Modulverantwortung
Prof. Dr.-Ing. Sebastian Biedermann

Dozierende
Prof. Dr.-Ing. Sebastian Biedermann

Verwendbarkeit	BISD
Studiensemester	2. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
keine

Inhalte
Die Studierenden lernen den Beruf des Penetration-Testers/-in bzw. Security-Researchers/-in mit den dazugehörigen Rahmenbedingungen und Vorgehensweisen kennen.
In diesem Zusammenhang liegt der Fokus auf dem Identifizieren, Verstehen und Ausnutzen von gängigen Schwachstellen in IT-Systemen.

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch/Englisch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Die Studierenden können nach Abschluss des Moduls:

- das Berufsbild von Penetration-Testern bzw. Security-Researchern beschreiben und deren Aufgaben im Kontext der IT-Sicherheit erläutern.
- den typischen Ablauf eines Penetration-Tests – von der Informationsbeschaffung bis zum Reporting – systematisch darstellen.
- rechtliche Rahmenbedingungen und ethische Aspekte von Penetration Tests benennen und bei der Durchführung berücksichtigen.
- häufige Schwachstellen in Webanwendungen, klassischen Anwendungen, Protokollen und Hardware-Komponenten erkennen und praktisch ausnutzen.
- Schwachstellen mit gängigen Tools (z. B. Burp Suite, Metasploit) identifizieren und deren Auswirkungen technisch fundiert bewerten.
- Post-Exploitation-Techniken anwenden, um Zugriff auf Systeme zu erweitern oder zu vertiefen (z. B. Credential Dumping, Privilege Escalation).
- Methoden des Lateral Movement beschreiben und exemplarisch durchführen, um sich innerhalb eines Netzwerks weiterzubewegen.
- identifizierte Schwachstellen hinsichtlich ihres Risikopotenzials einschätzen und priorisieren (z. B. mithilfe von CVSS).
- die Ergebnisse eines Penetration-Tests in einem strukturierten Report dokumentieren und zielgruppengerecht präsentieren.
- die Grenzen und Risiken von Penetration Testing reflektieren, insbesondere im Hinblick auf unbeabsichtigte Auswirkungen und Haftungsfragen.

Literatur
The Web Application's Hackers Handbook (Dafydd Stuttart et al.), 2023
Penetration Testing - a Hands-On Introduction to Hacking (Georgia Weidman), 2014
Hacking, The Next Generation (Nitesh Dhanjani et al.), 2021

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 5000220,5100220,6810080 Programmieren II

Modulprofil

Prüfungsnummer
5000220,5100220,6810080

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Semester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht, Übung

Lehrsprache
Deutsch

Organisation

Modulverantwortung
Prof. Dr. Steffen Heinzl

Dozierende
Prof. Dr. Steffen Heinzl, Christine Zilker

Verwendbarkeit	BIN, BISD, BWI
Studiensemester	2. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
bZv

Empfohlene Voraussetzungen
Programmieren I

Inhalte
Im Modul Programmieren II geht es darum, die objektorientierte Programmierung (in der Programmiersprache Java) zu erlernen. Um größere Informationssysteme zu strukturieren, ist es wichtig zu lernen, wie diese aufgebaut, designed und getestet werden können.

Dieser Kurs besteht aus 13 Lektionen, die aus Lernvideos, den dazugehörigen Übungen, den Power-Point-Folien zu den Videos und zum Stoff passenden Quizzen bestehen.

Die Lernvideos sind so strukturiert, dass die Studierenden zunächst mit Tests konfrontiert werden und danach nach und nach Objektorientierung und deren Anwendung erlernen. Der begleitende Seminaristische Unterricht dient dem Stellen von Fragen und der Vertiefung des Stoffs.

Die Übungen sind der mit Abstand wichtigste Bestandteil des Kurses. Durch das eigenständige Lösen von Problemstellungen erlernen die Studierenden die objektorientierte Programmierung. Die Übungstermine helfen, indem Studierenden dort vom Dozenten Denkanstöße gegeben werden, wenn ein Studierender bei Aufgaben nicht weiterkommt, und die Qualität von Lösungen besprochen und verbessert werden. Die Übungen gehören in der Regel zu den vorherigen Lernvideos und greifen deren Inhalte auf.

Zu jeder Lektion gibt es ein Quiz, das durch einfache Fragen den Studierenden eine Überprüfungsmöglichkeit gibt, ob sie den behandelten Stoff wissen bzw. verstehen.

Inhalte:
Unit Tests (JUnit 5)
Dependency Management (Maven)
Vererbung (Spezialisierung, Generalisierung)
Enumerations
Abstrakte Klassen, Interfaces, Komposition
Exceptions
Streams
Generics
Collections, Assoziative Arrays (Maps)
Geschachtelte Klassen (static nested, inner, local, anonymous classes)

Lambda-Ausdrücke
Threads
Design Patterns: Builder, Decorator, Visitor
Fluent Interfaces
Funktionale Programmierung mit Hilfe der Stream-API

IDE: Eclipse oder IntelliJ

Die Inhalte und erworbenen Kompetenzen dieses Moduls erleichtern die Module Programmieren 3 und das Programmierprojekt deutlich und sind nützlich für

- Mathematische SW in der Informatik
- Algorithmen und Datenstrukturen 2
- Betriebssysteme
- Grundlagen Verteilte Systeme
- Datenmanagement & Data Science

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Nach dem erfolgreichen Abschluss des Moduls sind die Studierenden in der Lage

- Konzepte der objektorientierten Programmierung anzuwenden
- eigenständig eine Lösungsstrategie zum Schreiben objektorientierter Java-Programme umzusetzen
- Teillösungen von größeren Programmen/Problemstellungen zu implementieren
- Probleme in mehrere Teilprobleme zu strukturieren
- Tests für Softwaresysteme zu implementieren
- Polymorphie bei Methoden und Typen zu verstehen und einzusetzen
- Klassenbibliotheken zur Erweiterung von Programmen einzusetzen
- erste Design Patterns zu verstehen

Literatur
Schiedermeier, Reinhard: Programmieren mit Java. Pearson, 2. Auflage, 2010.
Schiedermeier, Reinhard: Programmieren mit Java II. Pearson, 2013.
Bloch, Joshua: Effective Java. 3rd Edition, Addison-Wesley, 2017.
Ullenboom, Christian: Java ist auch eine Insel. 16. Auflage, Rheinwerk Computing, 2021.

3. Semester

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 5111160,6810140
Backend Systems

Modulprofil

Prüfungsnummer
5111160,6810140

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Wintersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 30 Std.

Selbststudienzeit: 120 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht

Lehrsprache
Englisch

Organisation

Modulverantwortung
Prof. Dr. Peter Braun

Dozierende
Prof. Dr. Peter Braun

Verwendbarkeit	BIN, BISD
Studiensemester	3. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
None

Empfohlene Voraussetzungen
Programmieren 1 und Programmieren 2

Inhalte

- Introduction to distributed systems, client-server, and peer-to-peer systems.
- Software architectures for backend systems (3-tier, hexagonal, monolithic vs. micro-service, event-driven)
- Frameworks to implement backend systems (e.g. Spring)
- Advanced database techniques, scalability, replication, sharding, ORM-tools, query caching, CAP theorem
- Protocols for remote procedure call, for example, GraphQL and Google RPC.
- Basics of the HTTP protocol and application in the form of Web APIs.
- Comprehensive introduction to the REST architecture principle: resources, URLs, CRUD, hypermedia, caching, security.
- Configuration of Web servers (Apache), load balancer, and public caches (nginx)
- Testing of backend systems, performance testing using JMeter, monitoring and logging
- Security aspects of network protocol and backend systems

In the traditional degree programme, the lecturer provides or agrees with the topics of the practical examples for the examination. In the BIN dual study programme, the lecturer consults with the company on a task, ensuring practical relevance and feedback from the company.

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Sonstige Prüfung (soP) gemäß §§ 26, 27 APO

Dauer/Form der Prüfung
Portfolio

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Englisch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse

- The students understand the fundamental concepts and differences of distributed systems, including their architecture and communication models.
- The students analyze various software architectures for backend systems and evaluate their suitability for different use cases.
- The students apply advanced database techniques such as replication and sharding to enhance data availability and performance.
- The students implement a backend system using a framework like Spring, following best practices for configuration, deployment, and security.
- The students compare different protocols for remote procedure calls, such as GraphQL and Google RPC, assessing their strengths and limitations.
- The students design RESTful APIs by applying the principles of the REST architecture, focusing on resources, URLs, CRUD operations, and security strategies.
- The students evaluate the security aspects of network protocols and backend systems, proposing improvements based on best practices.

Literatur

- Coulouris, J. Dollimore, and T. Kindberg, Distributed Systems: Concepts and Design (4th Edition) (International Computer Science). Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2005.
- N. Biswas, Practical GraphQL: Learning Full-Stack GraphQL Development with Projects. Berkeley, CA: Apress, 2023.
- J. Webber, S. Parastatidis, and I. Robinson, REST in practice: hypermedia and systems architecture, 1. ed. in Theory in practice. Beijing Köln: O'Reilly, 2010.
- L. Richardson and M. Amundsen, RESTful Web APIs, First edition, Second release. Beijing Cambridge Farnham Köln Sebastopol Tokyo: O'Reilly, 2015.
- I. Dominte, Web API Development for the Absolute Beginner: A Step-by-step Approach to Learning the Fundamentals of Web API Development with .NET 7. Berkeley, CA: Apress, 2023.

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 6810180
Governance, Risk, Compliance and Ethics

Modulprofil

Prüfungsnummer
6810180

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Wintersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht

Lehrsprache
Deutsch

Organisation

Modulverantwortung
Prof. Dr. Kristin Weber

Dozierende
Prof. Dr. Kristin Weber,
Prof. Dr. Markus Oermann

Verwendbarkeit	BISD
Studiensemester	3. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
ISM-Standards & Processes

Inhalte
Am Management von Informationssicherheit sind viele Personen und Einheiten in und außerhalb von Organisationen beteiligt. Governance regelt durch das Festlegen von Strukturen, Verantwortlichkeiten und Rahmenbedingungen wie Transparenz, Rechenschaftspflicht und Effizienz gewährleistet und gleichzeitig die Interessen aller Stakeholder gewahrt werden. Dieses Modul zeigt, welche Stakeholder das Informationssicherheitsmanagement hat, wie Verantwortlichkeiten festgelegt, Entscheidungen getroffen und optimale Rahmenbedingungen für maximale Informationssicherheit geschaffen werden.

Die Identifikation und Bewertung von IT-Risiken hilft Organisationen bei der gezielten und strukturierten Behandlung von Bedrohungen für die Informationssicherheit. Der risikoorientierte Ansatz wird in vielen ISMS-Rahmenwerken (Informationssicherheitsmanagementsystem) verfolgt. Das Modul vermittelt Grundlagen des IT-Risikomanagements, wie Maßnahmen zur Identifikation, Analyse, Bewertung und Behandlung von IT-Risiken in einem strukturierten Risikomanagementprozess.

Im Abschnitt zu Ethik werden essenzielle begriffliche Grundlagen der Moralphilosophie erläutert. Auf der Grundlage etablierter Schulen der Ethik wird die normative Begründung von (Informations-)Sicherheit als Wert und handlungsleitendes Prinzip beleuchtet. Die Betrachtung von Modellen für die Integration ethischer Überlegungen in Entwicklungs- und Systemdesignprozesse schlägt die Brücke zur Anwendung der ethischen Grundsätze in der Praxis. Für diese sind zudem Fragen der Compliance mit dem geltenden Datenschutzrecht von besonderer Relevanz. Nach einem Überblick über dessen Grundstrukturen liegt der Schwerpunkt auf den Anforderungen an den technischen und organisatorischen Datenschutz sowie der Durchsetzung und den Folgen von Rechtsverstößen. Abschließend werden Grundlagen des reformierten Informationssicherheitsrechts erläutert.

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Die Studierenden können nach Abschluss des Moduls:

- grundlegende Governance-Mechanismen (z. B. Verantwortlichkeiten, Leitlinien, Entscheidungsprozesse, Gremien) im Kontext der Informationssicherheit benennen und gezielt ausgestalten.
- relevante Rollen und Beteiligte im Informationssicherheitsmanagement innerhalb und außerhalb von Organisationen beschreiben und deren Aufgaben differenziert darstellen.
- die Bedeutung und Funktion von IT-Risikomanagement für die Informationssicherheit erklären und anhand praktischer Beispiele veranschaulichen.
- die organisatorischen Rahmenbedingungen für wirksames IT-Risikomanagement identifizieren und beschreiben.
- einen einfachen, strukturierten IT-Risikomanagementprozess nachvollziehen, anwenden und dokumentieren.
- ethische Herausforderungen im Umgang mit digitalen Systemen mit Sicherheitsrelevanz erkennen und Lösungsansätze zur Integration ethischer Prinzipien in Arbeitsprozesse entwickeln.
- die Grundstrukturen des Datenschutzrechts erläutern und grundlegende Fragen zur Datenschutz-Compliance beantworten.
- die wesentlichen Inhalte des Informationssicherheitsrechts beschreiben und deren Relevanz für die betriebliche Praxis bewerten.
- in datenschutz- und informationssicherheitsrechtlichen Fragestellungen zielgerichtet mit juristischen oder regulatorischen Expertinnen und Experten kommunizieren.
- die Zusammenhänge zwischen Governance, Risiko- und Compliance-Management sowie Ethik in sicherheitskritischen IT-Umgebungen reflektieren.

Literatur
Harich, T.: IT-Sicherheitsmanagement: das umfassende Praxis-Handbuch für IT-Security und technischen Datenschutz nach ISO 27001. 3. Auflage, MITP, 2021.
Johannsen, A.; Kant, D.: IT-Governance, Risiko- und Compliance-Management (IT-GRC) – Ein Kompetenz-orientierter Ansatz für KMU. In: HMD – Praxis der Wirtschaftsinformatik, 57, 2020, S. 1058-1074. https://doi.org/10.1365/s40702-020-00625-8
Kersten, H. et al.: IT-Sicherheitsmanagement nach der neuen ISO 27001 – ISMS, Risiken, Kennziffern, Controls. 2., aktualisierte Auflage, SpringerVieweg, 2020.
Lang, M.; Löhr, H.: IT-Sicherheit – Technologien und Best Practices für die Umsetzung in Unternehmen. 2., überarbeitete Auflage, Hanser, 2024.
Lewinski/Rüpke/Eckhardt (2022): Datenschutzrecht. 2. Auflage. München, C.H. Beck.

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 5003230,6810160
IT-Projektmanagement

Modulprofil

Prüfungsnummer
5003230,6810160

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Wintersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht, Übung

Lehrsprache
Deutsch

Organisation

Modulverantwortung
Prof. Dr.-Ing. Anne Heß

Dozierende
Prof. Dr. Eva Wedlich,
Prof. Dr.-Ing. Anne Heß

Verwendbarkeit	BISD, BWI
Studiensemester	3. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
keine

Inhalte
- Einführung Projekt und Projektmanagement
- Projektorganisation
- Projektplanungsprozess
- Projektkalkulation
- Projektsteuerung und –überwachung
- Projektabschluss
- Personalmanagement und Projektmarketing
- IT-Produktmanagement
- Kernaktivitäten in IT Projekten (Analyse, Design, Implementierung, Integration und Stabilisierung)
- Qualitätsmanagement und Qualitätssicherung
- Konfiguationsmanagement (rudimentär)
- Vorgehensmodelle (Phasenmodelle vs. Iterativ / Inkrementelle / agile Vorgehensmodelle)
- Agiles Projektmanagement / Scrum

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse

- Die Studierenden erlernen Projektmanagement-Kompetenzen, insbesondere die notwendigen Kenntnisse für Projektleiter/-innen. Hierzu werden Projektmanagement-Methoden, -Prozesse und -Hilfsmittel behandelt.
- Die Studierenden kennen relevante Kernaktivitäten der Softwareentwicklung und deren Zielsetzungen
- Die Studierenden können den Kernaktivitäten relevante Teilaktivitäten, Eingangsvoraussetzungen sowie Ergebnistypen zuordnen und beschreiben
- Die Studierenden können verschiedene Vorgehensmodelle (Wasserfall-Modell, V-Modell, Scrum) beschreiben, einschließlich deren jeweiligen Vor- und Nachteile und können Aktivitäten in den Vorgehensmodellen beschreiben und zuordnen
- Die Studierenden verstehen charakteristische Merkmale und Unterschiede zwischen phasen-orientierten Vorgehensmodellen und iterativen / inkrementellen Vorgehensmodellen und können geeignete Vorgehensmodelle für einen gegebenen Projektkontext auswählen und die Auswahl begründen
- Die Studierenden kennen die grundlegenden Prinzipien, Rollen, Artefakte, Zeremonien und Praktiken von Agilen Projekten (am Beispiel von Scrum) und können sich als Teammitglied in einem agilen Projekt zurechtfinden
- Die Studierenden verstehen die Bedeutung und Relevanz von Softwarequalität
- Die Studierenden kennen wesentliche Konzepte des Qualitätsmanagements und der Qualitätssicherung und können relevante Aufgaben und Fähigkeiten (Softskills) von Qualitätsbeauftragen beschreiben
- Die Studierenden kennen wesentliche Zielsetzungen, Konzepte und Aktivitäten des Konfigurationsmanagements, einschließlich grundlegender Funktionalitäten von Werkzeugen zur Unterstützung des Konfigurationsmanagements

Literatur

- Johannsen, A. und Kramer, A.: Basiswissen für Softwareprojektmanager, dpunkt.verlag, 2017.
- Olfert, K.: Projektmanagement, NWB Verlag, 11. Auflage 2019.
- Sterrer, C. und Winkler, G.: setting milestones. Projektmanagement (Methoden, Prozesse, Hilfsmittel), Goldegg Verlag, 2010.
- Sterrer, C.: pm k.i.s.s.: Keep it short and simple, Goldegg Verlag, 2011.
- Tiemeyer, E: Handbuch IT-Projektmanagement, Hanser 2018
- Ziegler, Michael : Agiles Projektmanagement mit Scrum für Einsteiger, ISBN-13: 979-8751100346 , 2021
- Gundlach, Marco: Agiles Projektmanagement- Erfolgreich navigieren mit Scrum und Kanban: Ein umfassender Leitfaden für Einsteiger und Experten, ISBN-13: 979-8392911936, 2023

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 6810170
Security Engineering

Modulprofil

Prüfungsnummer
6810170

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Wintersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht

Lehrsprache
Deutsch/Englisch

Organisation

Modulverantwortung
Prof. Dr.-Ing. Sebastian Biedermann

Dozierende
Prof. Dr. Benjamin Weggenmann,
Prof. Dr. Minal Moharir

Verwendbarkeit	BISD
Studiensemester	3. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
keine

Inhalte
Studierenden erwerben Kenntnisse und Fähigkeiten zur Konzeption und Analyse sicherer IT-Systeme unter Verwendung moderner kryptographischer Verfahren. Im Fokus steht die praktische Anwendung grundlegender kryptographischer Konzepte wie symmetrischer und asymmetrischer Verschlüsselung sowie Hashing-Algorithmen zur Entwicklung sicherer Anwendungen. Darüber hinaus befassen sich die Studierenden mit der Funktionsweise und sicherheitsrelevanten Aspekten zentraler Protokolle wie TLS, PGP, Kerberos, VPN/IPSec und dem Anonymisierungsnetzwerk TOR. Aktuelle Entwicklungen wie Post-Quantum-Kryptographie (z. B. Merkle Signature Scheme), Zero-Knowledge-Proofs sowie biometrische und Multi-Faktor-Authentifizierungsverfahren werden ebenfalls behandelt. Ein weiterer Schwerpunkt liegt auf dem Prinzip „Security by Design“ und der systematischen Identifikation sicherheitskritischer Schwachstellen in Systemarchitekturen. Die Studierenden lernen, sicherheitsrelevante Anforderungen zu analysieren und daraus robuste (verteilte) Systeme nach aktuellen Standards zu entwerfen. Das Modul vermittelt somit sowohl konzeptionelle als auch technische Kompetenzen zur Entwicklung sicherer Informationssysteme in komplexen Umgebungen.

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch/Englisch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Die Studierenden können nach Abschluss des Moduls:

- grundlegende kryptographische Konzepte (z. B. symmetrische/ asymmetrische Verschlüsselung, Hashing) beschreiben und in sicherheitsrelevanten Anwendungsszenarien gezielt einsetzen.
- die Funktionsweise sicherheitsrelevanter Protokolle wie TLS, Kerberos, VPN/IPSec, PGP oder TOR erklären und sicherheitskritische Schwachstellen analysieren.
- moderne Authentifizierungsverfahren wie Multi-Faktor-Authentifizierung, biometrische Verfahren und deren sicherheitstechnische Stärken und Schwächen beurteilen.
- die Grundlagen aktueller kryptographischer Entwicklungen wie Post-Quantum-Kryptographie (z. B. Merkle Signature Scheme) erläutern und deren Potenzial einschätzen.
- Anforderungen an sichere (verteilte) Systeme analysieren und systematisch in ein sicheres Systemdesign überführen.
- kryptographische Verfahren in den Entwurf sicherer Systeme und Protokolle integrieren und dabei aktuelle Standards und Best Practices berücksichtigen.
- potenzielle Bedrohungen im Design sicherheitsrelevanter Systeme erkennen und geeignete technische Gegenmaßnahmen konzipieren.
- Sicherheitseigenschaften (z. B. Vertraulichkeit, Integrität, Authentizität) in Systementwürfen systematisch berücksichtigen und evaluieren.
- den Zusammenhang zwischen technischer Implementierung, kryptographischen Grundlagen und sicherem Systemdesign reflektieren.

Literatur
Security Engineering: A Guide to Building Dependable Distributed Systems, Ross Anderson, 2020
Applied Cryptography: Protocols, Algorithms and Source Code in C, Bruce Schneider, 1996
Bulletproof TLS and PKI, Second Edition: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications, Ivan Ristic, 2022

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 5003031
Software industry, education and economy in India

Modulprofil

Prüfungsnummer
5003031

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Wintersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminar

Lehrsprache
Englisch

Organisation

Modulverantwortung
Prof. Dr. Isabel John

Dozierende
Prof. Dr. Isabel John,
Prof. Dr.-Ing. Erik Schaffernicht

Verwendbarkeit	BDGD, BEC, BIN, BISD, BWI
Studiensemester	3. Semester
Art des Moduls	FWPM

Verpflichtende Voraussetzungen gemäß SPO
Gute Englisch-Kenntnisse

Empfohlene Voraussetzungen
keine

Inhalte
Einführung in das Land Indien und unsere Partnerhochschule Christ University in Bangalore
Auswahl der Themen für die inter-kulturellen Präsentationen (z.B. Politik, Religion, IT-Industrie) in Vorbereitung auf die Exkursion.
Vorstellung von Methoden zur Entwicklung von Präsentationen hinsichtlich Themenauswahl, Gliederung und Foliengestaltung.
Einführung in das Thema für die gemeinsamen Projekte mit den Studierenden der Christ University, die ab Oktober in Kleingruppen bearbeitet werden.

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Sonstige Prüfung (soP) gemäß §§ 26, 27 APO

Dauer/Form der Prüfung
Portfolio

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Englisch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Die Studierenden erinnern grundlegende Fakten über das Land Indien und seine Bedeutung in der Informationstechnologie.
Die Studierenden analysieren und bewerten Unterschiede zwischen Deutschland und Indien.
Die Studierenden benutzen einen bild-orientierten freien Vortragsstil bei den Präsentationen.
Die Studierenden wenden grundlegende Kommunikationstechniken im inter-kulturellen Bereich am Beispiel Indien an.
Die Studierenden demonstrieren erfolgreiche Zusammenarbeit mit Studierenden der Partnerhochschule im Rahmen eines technischen Projektes.

Literatur
Wird im Seminar in Abhängigkeit von den Themen bekannt gegeben.

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 5111140,6820130 Systemnahe Programmierung

Modulprofil

Prüfungsnummer
5111140,6820130

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Wintersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht

Lehrsprache
Englisch

Organisation

Modulverantwortung
Prof. Dr. Peter Braun

Dozierende
Prof. Dr. Peter Braun

Verwendbarkeit	BIN, BISD
Studiensemester	3. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
None

Empfohlene Voraussetzungen
Programmieren I and Programmieren II

Inhalte
- Definition and meaning of system-oriented programming
- Using the command line of an operating system
- Shell programming using the example of Bash
- Data processing on the command line with sed, awk, sort, jq
- Using AI assistance systems (e.g. GitHub Copilot, ChatGPT)
- Editing text documents with vim
- Version control system Git
- Introduction to the C programming language (syntax, data types, pointers, memory management)
- System programming under Linux (system calls, handling files, processes)
- Security aspects of system-related programming and protection mechanisms
- Structure of the Linux operating system
- Processes, process management, scheduling
- Inter-process communication, race conditions, deadlocks, semaphores, Petri nets and deadlock detection, philosopher problem, producer-consumer problem
- Memory management, memory abstraction, partitioning, fragmentation, free memory management, virtual memory, page exchange algorithms
- Input and output, direct memory access, interrupts, hard disks, file systems for hard disks
- Network communication and implementation of network protocols
- Hypervisor technologies, Docker containers, resource management

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Sonstige Prüfung (soP) gemäß §§ 26, 27 APO

Dauer/Form der Prüfung
Portfolio

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Englisch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse

- The students understand the definition and principles of system-oriented programming, including its role in software development.
- The students demonstrate proficiency in using the command line of an operating system, applying advanced tools like sed, awk, sort, and jq for data processing tasks.
- The students develop shell scripts in Bash to automate system tasks and streamline operations effectively.
- The students utilize AI assistance systems, such as GitHub Copilot and ChatGPT, to improve coding efficiency and solve programming challenges.
- The students manage text documents using the vim text editor, employing advanced editing and configuration techniques.
- The students implement version control practices with Git to support collaborative software development workflows.
- The students program in C, focusing on syntax, data types, pointers, memory management, and use debugging and profiling tools like gdb, strace, ltrace, and gprof to analyze code performance.
- The students evaluate security aspects of system-related programming and apply protection mechanisms to ensure code security.

Literatur

- D. J. Barrett, Efficient Linux at the command line: boost your command-line skills, First edition. Sebastopol, CA: O'Reilly, 2022.
- A. S. Tanenbaum und H. Bos, Modern operating systems, 4. ed. Boston: Prentice Hall, 2015.
- K. Hitchcock, Linux System Administration for the 2020s: The Modern Sysadmin Leaving Behind the Culture of Build and Maintain. Berkeley, CA: Apress, 2022. doi: 10.1007/978-1-4842-7984-7.
- M. Kalin, Modern C Up and Running: A Programmer's Guide to Finding Fluency and Bypassing the Quirks. Berkeley, CA: Apress, 2022. doi: 10.1007/978-1-4842-8676-0.
- K. Hitchcock, The Enterprise Linux Administrator: Journey to a New Linux Career. Berkeley, CA: Apress, 2023. doi: 10.1007/978-1-4842-8801-6.
- J. Varma, Pro Bash: Learn to Script and Program the GNU/Linux Shell. Berkeley, CA: Apress, 2023. doi: 10.1007/978-1-4842-9588-5.
- S. M. Palakollu, Practical System Programming with C: Pragmatic Example Applications in Linux and Unix-Based Operating Systems. Berkeley, CA: Apress, 2021. doi: 10.1007/978-1-4842-6321-1.

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 6810150
Wirtschafts- und IT-Recht

Modulprofil

Prüfungsnummer
6810150

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Wintersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht

Lehrsprache
Deutsch

Organisation

Modulverantwortung
Prof. Dr. Oliver Ehret

Dozierende
Prof. Dr. Oliver Ehret

Verwendbarkeit	BISD
Studiensemester	3. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
keine

Inhalte
Allgemeines Vertragsrecht
Besonderes Vertragsrecht im Hinblick auf IT, spezielle Vertragstypen
Grundzüge des Urheberrechts
Überblick über relevante Bereiche des gewerblicher Rechtsschutz
Recht im Internet
Datenschutzrecht

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Einordnen von Recht, rechtlichen Grundbegriffen unseres Rechtssystems und dessen Grundstrukturen; Überblick, welche Rolle Recht für Informatiker spielt vermitteln. Wesentliche Grundlagen des allgemeinen Privat- und öffentlichen Rechts verstehen; IT-rechtliche Begriffe verstehen und einordnen; Überblick über die wesentlichen IT- relevanten Rechtsgebiete und vertraglichen Bereiche erhalten; Rechtliche Risiken erkennen, bewerten und begrenzen; Praxistaugliche Fertigkeiten im Umgang mit IT-relevanten rechtlichen Problemen entwickeln und grundlegende Vertragstypen im Bereich IT kennen; Urheberrechtliche Grundlagen, insbesondere im Bereich Software und Datenbanken erwerben, Grundsätze des Datenschutzes, insbesondere im Bereich IT verstehen.
Die Bedeutung des Datenschutzrechts, insbesondere auch im internationalen Zusammenhang, wird verdeutlicht. Hierbei wird auch Wert darauf gelegt zu vermitteln, wie eng Informatik, die Architektur von IT-Systemen, Informationssicherheit und Datenschutz verzahnt sind.

Literatur
Köhler, Bürgerliches Gesetzbuch, dtv, 89.Auflage 2022
Schneider: IT- und Computerrecht, 15. Auflage, Beck dtv, München 2022.
Kallwass, Abels: Privatrecht, Verlag Franz Vahlen München, 24. Auflage, 2021
Hoeren: IT Vertragsrecht, 2. Auflage, Verlag Otto Schmidt, Köln 2012.
Marly: Praxishandbuch Softwarerecht, 7. Auflage, C.H.Beck, München 2018.
Härting: Internetrecht, 7. Auflage, Verlag Otto Schmidt, Köln 2022.
Hoeren: Skript Internetrecht Uni Münster, Stand April 2020
Haug: Grundwissen Internetrecht, Verlag W. Kohlhammer, 3. Auflage, 2016
Redeker: IT-Recht, C.H.Beck, 7. Auflage, 2020
Schneider: Handbuch, EDV-Recht, Otto Schmidt, 5. Auflage, 2017
Kühling, Sack, Hartmann: Datenschutzrecht, 5. Auflage C.F.Müller, 2021

4. Semester

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 6810240
Expertise and Communication

Modulprofil

Prüfungsnummer
6810240

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Sommersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 30 Std.

Selbststudienzeit: 120 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminar

Lehrsprache
Deutsch/Englisch

Organisation

Modulverantwortung
Prof. Dr. Kristin Weber

Dozierende
Prof. Dr. Kristin Weber,
Prof. Dr.-Ing. Sebastian Biedermann

Verwendbarkeit	BISD
Studiensemester	4. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
Modul 6810060

Empfohlene Voraussetzungen
none

Inhalte
In diesem Seminar beschäftigen sich die Studierenden selbstständig mit aktuellen Themen aus allen Bereichen der Informationssicherheit und angrenzender Themengebiete, wie dem Datenschutz. Die Dozierenden geben eine Auswahl an Themenstellungen vor, aus denen die Studierenden sich ein Thema auswählen oder sie schlagen ein anderes Thema vor. Das gewählte Thema wird umfassend und nach wissenschaftlichen Grundsätzen eigenständig durch die Studierenden bearbeitet und in einer Hausarbeit dokumentiert. Das begleitende Seminar vermittelt Schreib- und Kreativitätstechniken sowie Grundlagen wissenschaftlicher Recherche und Arbeit. Zudem stellen die Studierenden ihre Themen in einer Präsentation für fachfremdes Publikum vor, um ihre Fähigkeiten der zielgruppengerechten Aufbereitung von technischen Themen zu erproben.

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Sonstige Prüfung (soP) gemäß §§ 26, 27 APO

Dauer/Form der Prüfung
Praktische Studienleistung

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch/Englisch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Nach erfolgreichem Abschluss dieses Moduls,

- wissen die Studierenden, wie sie sich selbstständig in Themen der Informationssicherheit einarbeiten und ihr Wissen erweitern.
- kennen sie weitere aktuelle Fragestellungen zu Informationssicherheit und angrenzender Themengebiete, z.B. Datenschutz.
- sind sie in der Lage Grundlagen des wissenschaftlichen Arbeitens anzuwenden.
- können die Studierenden Zwischenergebnisse zeigen, dokumentieren und diskutieren und wissen, welche Rolle Feedback im wissenschaftlichen Diskurs spielt.
- sind sie in der Lage, eine schriftliche Ausarbeitung zu erstellen, die wissenschaftlichen Maßstäben gerecht wird.
- können sie wissenschaftliche und technische Themen zielgruppengerecht aufbereiten, kommunizieren und präsentieren.
- kennen sie Schreib- und Kreativitätstechniken und können diese situationsbedingt anwenden.

Literatur
Aengenheyster, S.; Dörr, K. (Hrsg.): Praxishandbuch IT-Kommunikation. SpringerGabler, 2019.
Kirchem, S.; Waack, J.: Personas entwickeln für Marketing, Vertrieb und Kommunikation – Grundlagen, Konzept und praktische Umsetzung. SpringerGabler 2021.
Lubienetzki, U.; Schüler-Lubienetzki, H.: Was wir uns wie sagen und zeigen – Psychologie der menschlichen Kommunikation. Springer, 2020.

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 5111230,6810200
Frontend Systems

Modulprofil

Prüfungsnummer
5111230,6810200

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Sommersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht, Übung

Lehrsprache
Englisch

Organisation

Modulverantwortung
Prof. Dr. Peter Braun

Dozierende
Prof. Dr. Peter Braun

Verwendbarkeit	BIN, BISD
Studiensemester	4. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
none

Empfohlene Voraussetzungen
Backend Systems

Inhalte

- Introduction to Web Technologies: Basic building blocks of web development, including HTML for structuring web content, CSS for styling and layout, and JavaScript for adding interactivity and dynamic behavior to web pages.
- Advanced JavaScript and Modern ES6+ Features: More details about JavaScript, exploring modern ES6+ features such as let, const, arrow functions, template literals, modules, promises, and async/await, and learn how to apply these in real-world scenarios.
- Fundamentals of React: Core concepts of React, including its component-based architecture, JSX syntax, and the use of state and props to manage data within components, enabling the creation of dynamic and interactive user interfaces.
- Advanced React Techniques: Advanced topics in React, such as the Context API for state management across the application, React hooks for managing state and side effects in functional components, and performance optimization strategies.
- IT Security in Frontend Development: Principles of IT security as they relate to frontend development, including securing user input, preventing cross-site scripting (XSS) and cross-site request forgery (CSRF), and ensuring secure communication between frontend and backend systems. Introduction to the Open Web Application Security Project Top Ten list.
- Project Development and Deployment: Setting up development environments, following best practices in code organization and documentation, and deploying and maintaining frontend applications in a production environment.

In the traditional degree programme, the lecturer provides or agrees with the topics of the practical examples for the examination. In the BIN dual study programme, the lecturer consults with the company on a task, ensuring practical relevance and feedback from the company.

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Sonstige Prüfung (soP) gemäß §§ 26, 27 APO

Dauer/Form der Prüfung
Portfolio

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Englisch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse

- The students understand the foundational principles of HTML, CSS, and JavaScript to build and style basic web pages effectively.
- The students apply modern web frameworks like React and Svelte to develop dynamic and responsive user interfaces.
- The students analyze different state management techniques, such as React hooks and the context API, to manage complexity in web applications.
- The students design cross-platform mobile user interfaces using Flutter, focusing on user experience and performance.
- The students implement best practices in frontend development, including version control, testing, and secure deployment processes.
- The students create a comprehensive frontend project from scratch, integrating all learned concepts into a fully functional application.
- The students evaluate different frameworks and tools for frontend development to make informed decisions based on specific project requirements.

Literatur

Marijn Haverbeke: Eloquent JavaScript: A Modern Introduction to Programming. 4th edition, 2024.
Alex Banks, Eve Porcello: Learning React: Modern Patterns for Developing React Apps. O'Reilly, 2020.
Thomas Bailey, Alessandro Biessek: Flutter for Beginners: Cross-platform mobile development from Hello, World! to app release with Flutter 3.10+ and Dart 3.x. Packt, 2023.
Andrew Hoffman: Web Application Security: Exploitation and Countermeasures for Modern Web Applications. O'Reilly, 2024.

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 6100930,6810190 Innovationsmanagement und Unternehmensgründung

Modulprofil

Prüfungsnummer
6100930,6810190

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Sommersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht

Lehrsprache
Deutsch

Organisation

Modulverantwortung
Prof. Dr. Michael Müßig

Dozierende
Prof. Dr. Michael Müßig

Verwendbarkeit	BEC, BISD
Studiensemester	4. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
keine

Inhalte
Intro: Motivation, Innovation, Unternehmen, Unternehmensgründung, Startup und ein Blick in die Wirtschaftsgeschichte
Definitionen: Management, .. und alle Begriffe rund um Innovation und Innovationsarten
Prozesse und Zusammenhänge: Adoption und Diffusion, Akzeptanz
Vorhersage: Gartner´s Hypecycle und die three horizons
Innovation im Unternehmen, Schumpeter und the innovator´s dilemma, Disruption
Startup Ökosysteme
End-to-End: Design Thinking, Personas und Value Proposition, Business Model Canvas, Lean Startup und Customer Develpoment, MVP und Prototyping
Der Business Plan, Gründerteam
Wachsen und Wandel, Growth Hacking
Unternehmen gründen, finanzieren, gestalten und bewerten
Open und Crowd Innovation, Jugaad, Frugal und Nachhaltigkeit beim Gründen und bei Innovationen

CASE-Studies (wechselnd): Tesla, Kodak und die Digitalfotografie, Fashion and TEC, Scoutbee, Vogel Communications

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Nach erfolgreicher Teilnahme am Modul sind die Studierenden in der Lage:

- Die Begrifflichkeiten im Umfeld Innovationsmanagement und auch der Unternehmensgründung und -führung darstellen und erklären zu können
- Aussagen zu regionalen und unternehmensinternen Ökosystemen für Innovation und Intra- und Entrepreneurship zu beurteilen
- Die Bedeutung von Teams, Teamprozessen im Bereich der Innovationsentwicklung und der Unternehmensgründung zu verstehen und teambildende Methoden anwenden zu können
- Die Studierenden lernen die Grundlagen eines Businessplanes in seiner Struktur und seiner Entstehung kennen und können eigenständig einen solchen entwickeln und erstellen
- Die wesentlichen steuerlichen, rechtlichen und wirtschaftlichen Bausteine einer erfolgreichen Unternehmensgründung benennen und in ihrer Bedeutung analysieren
- Mit Hilfe der methodischen Herangehensweisen an Design Thinking, Value Propostion und Business Model können eigene Geschäftsmodellideen dargestellt und entworfen werden

Literatur
Verpflichtend:
Hess, Thomas: Digitale Transformation strategisch steuern. Springer Fachmedien Wiesbaden GmbH, 2019
Osterwalder, Alexander; Pigneur, Yves u.a.: Business Model Generation, campus Verlag, 2013 (und neuere Auflagen)
Ries, Eric: Lean Startup, 4. Aufl. Reline-Verlag München 2015
Kotsemir, M.; Abroskin, A.; Meissner, D.: Innovation Concepts and Typology - an evolutionary
Discussion. Basic Research Program, Working papers, SERIES: SCIENCE, TECHNOLOGY AND INNOVATION WP BRP 05/STI/2013

Ergänzend:
Christensen, Clayton M.: The Innovators Dilemma, Harvard Business Review Press (1997 und aktuelle Auflagen, auch in deutsch erhältlich)
Burkhardt, Christoph: Denkfehler Innovation; SpringerGabler 2017

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 5100240,6810210
Programmierprojekt

Modulprofil

Prüfungsnummer
5100240,6810210

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Semester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 12 Std.

Selbststudienzeit: 138 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminar

Lehrsprache
Deutsch

Organisation

Modulverantwortung
Prof. Dr. Peter Braun

Dozierende
Prof. Dr. Peter Braun

Verwendbarkeit	BISD, BIN
Studiensemester	4. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
BIN: Programmieren I und Programmieren II
BISD: Programmieren I

Empfohlene Voraussetzungen
Programmieren I + II
Datenbanken I
Software Engineering I

Inhalte
Die Studierenden sollen in Gruppen eine eigene Anwendung umsetzen. Eine Anwendung könnte bspw. ein Spiel, eine Three-Tier-Webanwendung oder eine vergleichbare Anwendung sein. Mögliche Anwendungsteile wären dabei eine grafische Oberfläche (auch Weboberfläche), Datenbankanbindung inkl. Schemaentwurf, Netzwerkkommunikation, KI, etc.
Weiterhin erstellen die Studenten eine Dokumentation (Gesamtüberblick, verschiedene Anwendungsfälle, die wichtigsten Aktivitäts- und Sequenzdiagramme, etc.).

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Sonstige Prüfung (soP) gemäß §§ 26, 27 APO

Dauer/Form der Prüfung
Praktische Studienleistung

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Nach dem erfolgreichen Abschluss des Moduls sind die Studierenden in der Lage

- eine erste größere Anwendung in einem Team von 4-6 Personen zu entwickeln
- eine Projektplanung durchzuführen und umzusetzen
- eine Aufgabenverteilung durchzuführen und umzusetzen
- Kenntnisse über den Softwareentwurf anzuwenden
- gelernte Programmierkonzepte anzuwenden
- mit passender Literatur benötigte Inhalte selbst nachzuschlagen
- eine Aufgabenstellung in Teilprobleme zu zerlegen.

Literatur
Keine

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 6810220
Rechnerarchitektur

Modulprofil

Prüfungsnummer
6810220

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Sommersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht, Übung

Lehrsprache
Deutsch

Organisation

Modulverantwortung
Prof. Dr. Christian Bachmeir

Dozierende
Prof. Dr. Christian Bachmeir

Verwendbarkeit	BISD
Studiensemester	4. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
Grundlagen der Technischen Informatik

Inhalte
- Historische Entwicklung
- Rechnerklassifikationen (Flynn, Händler, Giloi)
- Rechnerarithmetik (Darstellung von Zeichen und Zahlen, IEEE 745, Grundrechenarten, Booth Algorithmus)
- Mikrorechnerkern mit Steuer- und Rechenwerk (Pipelinekonzept, Dependenzen und deren Auflösung, Dynamisches Scheduling: Scoreboard, Tomasulo)
- Maschinenbefehle (ISA, Adressierungsarten, Assemblerprogrammierung)
- x86 Assembler (nasm, Linux/Ubuntu)
- RISC / CISC Konzepte (Ressourcenkonflikte, µProgrammierung)
- Speicher (Aufbau DRAM, SRAM, Caches, Kohärenzprotokolle)
- I/O und Peripherie (Externe Speicher, Busse)
- Parallelrechner und Multithreading
- Leistungsbewertung (Grundbegriffe, Benchmarks)

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Schriftliche Prüfung (sP) gemäß § 23 APO

Dauer/Form der Prüfung
90 Minuten

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Die Studierenden erlangen ein Verständnis vom Aufbau und der Arbeitsweise von Rechenanlagen,
und der Arbeitsweise verschiedener Rechnerarchitekturen.
Dazu kommen grundsätzliche Kenntnisse im Bereich Embedded Systems.
.
Die Studierenden sind in der Lage,

- Grundkomponenten einfacher Rechner darzustellen,
- verschiedene Realisierungsformen komplexer Schaltungen zu erläutern,
- relevante Speichertechnologien zu beschreiben,
- Aufbau und Programmierung von Prozessoren zu analysieren,
- einfache Assemblerprogramme zu implementieren und dabei spezifische Eigenschaften eines Rechners bei der Programmierung zu berücksichtigen,
- Leistungsfähigkeit von Rechnern zu bewerten,
- Teilkomponenten eines einfachen Rechnern zu entwerfen.

Literatur
J. Hennessy, D. Patterson: Computer Architecture, A Quantitative Approach, 2017
J. Hennessy, D. Patterson: Computer Organization and Design, 2022
U. Brinkschulte, T. Ungerer: Mikrocontroller und Mikroprozessoren, 2002
A. Tanenbaum: Structured Computer Organisation, 2021
W. Coy: Aufbau und Arbeitsweise von Rechenanlagen, 1992
P. Hermann: Rechnerarchitektur, 2013
H. Bähring: Mikrorechner-Systeme, 1994
C. Märtin: Einführung in die Rechnerarchitekturen, 2003
H. Malz: Rechnerarchitektur, 2004
W. Oberschelp, G. Vossen: Rechneraufbau und Rechnerstrukturen, 2006
B. Bundschuh, P. Sokolowsky: Rechnerstrukturen und Rechnerarchitekturen, 1996
Todd Austin Andrew S. Tanenbaum. Rechnerarchitektur: Von der digitalen Logik zum Parallelrechner. Pearson, 2014
John L. Hennessy David A. Patterson. Computer Organization and Design: The Hardware/Software Interface. Morgan Kaufmann Publishers, 1994
Matthias Homeister. Quantum Computing verstehen: Grundlagen-Anwendungen-Perspektiven. Springer-Verlag, 2022
Vossen Oberschelp. Rechnerarchitektur. Oldenbourg-Verlag, 2006
Grundlagen der Rechnerarchitektur, Frank Slomka, Michael Glaß, Springer, 2023
Grundkurs Informatik, Ernst, Schmidt, Beneken, Springer, 2023

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 6810230
Security Operations

Modulprofil

Prüfungsnummer
6810230

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Sommersemester

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht

Lehrsprache
Deutsch/Englisch

Organisation

Modulverantwortung
Prof. Dr.-Ing. Tobias Fertig

Dozierende
Prof. Dr.-Ing. Tobias Fertig, Dr.-Ing. Rodrigo Daniel do Carmo

Verwendbarkeit	BISD
Studiensemester	4. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
keine

Empfohlene Voraussetzungen
keine

Inhalte
Studierenden lernen Netzwerke und IT-Systeme mithilfe technischer Schutzmaßnahmen abzusichern. Dabei stehen zentrale Sicherheitskomponenten wie Firewalls, Proxies und Intrusion-Detection-Systeme (IDS) im Fokus. Die Studierenden erwerben praktische Kenntnisse zur Einrichtung, Konfiguration und Anwendung dieser Systeme in realitätsnahen Szenarien. Die Inhalte orientieren sich an typischen Anforderungen eines Unternehmensumfelds sowie an etablierten Sicherheitsstandards wie denen des National Institute of Standards and Technology (NIST). Ein besonderer Schwerpunkt liegt auf dem Thema Security-Monitoring: Die Studierenden lernen, sicherheitsrelevante Informationen aus verschiedenen Quellen zu identifizieren, zu korrelieren und zielgerichtet auszuwerten. Sie entwickeln und implementieren fallspezifische Erkennungsregeln zur Angriffserkennung und befassen sich mit den Aufgaben und Prozessen eines Security Operations Centers (SOC), einschließlich Logging, Incident Detection und Response. Das Modul vermittelt somit ein praxisnahes Verständnis für den operativen Betrieb von IT-Sicherheitssystemen in modernen Unternehmensumgebungen.

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Sonstige Prüfung (soP) gemäß §§ 26, 27 APO

Dauer/Form der Prüfung
Praktische Studienleistung

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch/Englisch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse

- Studierende kennen die Funktionen von Firewalls, Proxies und Intrusion-Detection-Systemen und können diese einrichten
- Studierende können fallspezifische Regeln zur Erkennung von Angriffen entwickeln und umsetzen
- Studierende können sicherheitsrelevante Information zum Security-Monitoring identifizieren und zusammenführen
- Studierende kennen die Aufgaben eines Security Operations Centers (SOC)

Literatur

Defensive Security Handbook: Best Practices for Securing Infrastructure, Lee Brotherston und Amanda Berlin, 2017
Zero Trust Security: An Enterprise Guide, Jason Garbis und Jerry W. Chapman, 2021
Security Operations Center: Building, Operating and Maintaining Your SOC, Joseph Muniz und Gary McIntyre, 2015

5. Semester

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 6810250
Praxismodul

Modulprofil

Prüfungsnummer
6810250

Dauer
1 Semester

Häufigkeit des Angebots
Jedes Semester

SWS
1

ECTS-Credits (CP)
30.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 15 Std.

Selbststudienzeit: 885 Std.

Gesamt: 900 Std.

Lehrveranstaltungsart(en)
Praxis

Lehrsprache
Deutsch/Englisch

Organisation

Modulverantwortung
Michael Rott

Dozierende
Michael Rott

Verwendbarkeit	BISD
Studiensemester	5. Semester
Art des Moduls	Pflichtmodul

Verpflichtende Voraussetzungen gemäß SPO
> 90 ECTS-Punkte. 55 ECTS aus 1.Jahr

Empfohlene Voraussetzungen
keine

Inhalte
- Im Rahmen eines größeren IT-Projektes ist die eigenverantwortliche Mitarbeit in möglichst allen Projektphasen (Systemanalyse, Systemplanung, Implementierung, Systemeinführung und Test) sicherzustellen. Dieses Projekt soll einen zeitlichen Umfang von mind. 12 Wochen haben.
- Optimalerweise lernt die Praktikantin/der Praktikant vor dem Projekt verschiedene Abteilungen und Bereiche des Unternehmens kennen, um ein grobes Verständnis für andere Abteilungen sowie das Unternehmen als Ganzes zu erlangen.

Ansprechpartner/Betreuer an der FHWS ist der Beauftragte für die begleitete Praxisphase, Prof. Dr. Tobias Aubele

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Sonstige Prüfung (soP) gemäß §§ 26, 27 APO

Dauer/Form der Prüfung
Dokumentation, Präsentation

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Deutsch/Englisch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Die Praktikantin/der Praktikant soll

- einschlägige, praxisorientierte Kenntnisse betrieblicher Abläufe erwerben
- (durch Anleitung) lernen, selbständig und eigenverantwortlich in IT-Projekten zu arbeiten.
- im Studium erworbene Kompetenzen mit den Erfahrungen der Praxis verknüpfen.
- lernen, Probleme und Anforderungen (bspw. Kundenwünsche) zu verstehen.
- lernen, Problemlösungen (bspw. für Unternehmensprozesse und/ oder IT-Projekte) zu konzipieren und zu implementieren.
- die Arbeit im Team erleben.
- die Einbettung in das Unternehmen, dessen Prozesse und organisatorische Abläufe kennen und erleben lernen.
- das Berufsfeld des Informatikers kennen und erleben lernen.
- lernen, bei Problemen auf die richtigen Ansprechpartner zuzugehen.
- den unbedingten Willen zur erfolgreichen und professionellen Umsetzung von Projekten vorgelebt bekommen.
- Exzellenz und Professionalität erleben.
- erleben, wie Mitarbeiterinnen und Mitarbeiter mit in den Bann gezogen werden.
- den Sinn ihrer/seiner Tätigkeit erkennen und fühlen.

Literatur
keine allgemeine Literaturempfehlung möglich

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

7. Semester

fiw.thws
Fakultät Informatik und Wirtschaftsinformatik
Technische Hochschule Würzburg-Schweinfurt

Modul: 5003198
Green IT (Blended Intensive Program)

Modulprofil

Prüfungsnummer
5003198

Dauer
1 Semester

Häufigkeit des Angebots
Unregelmäßig

SWS
4

ECTS-Credits (CP)
5.0

Workload
Angeleitete Studienzeit:
Präsenzzeit: 60 Std.

Selbststudienzeit: 90 Std.

Gesamt: 150 Std.

Lehrveranstaltungsart(en)
Seminaristischer Unterricht

Lehrsprache
Englisch

Organisation

Modulverantwortung
Prof. Dr. Peter Braun

Dozierende
Prof. Dr. Peter Braun,
Prof. Dr. Frank-Michael Schleif

Verwendbarkeit	BIN, BWI, BEC, BISD, BDGD
Studiensemester	7. Semester
Art des Moduls	FWPM

Verpflichtende Voraussetzungen gemäß SPO
None

Empfohlene Voraussetzungen
None

Inhalte
This module explores how sustainability principles can be integrated into the design, development, deployment, and management of IT systems. It offers a multidisciplinary perspective on the environmental, economic, and societal implications of information technology. Through lectures, case studies, and collaborative international projects, students gain both theoretical foundations and practical experience in Green IT strategies. Partnering with universities in the Czech Republic, Germany, and Iceland, the module includes cross-border collaboration and comparative analysis of regional IT sustainability approaches. This module contains a compulsory study trip to Prague, the Czech Republic.

- Introduction to Green IT: Definition, significance, and global relevance; real-world applications in industry and academia
- Environmental Impact of IT: Carbon footprint, e-waste, lifecycle analysis, and Green Computing standards
- Sustainable Software Engineering: Design principles and code optimization for energy efficiency
- Green Algorithms and Data Structures: Techniques to reduce energy consumption and benchmark software for efficiency
- AI and Machine Learning for Green IT: Optimization of energy use, environmental monitoring, and ethical implications
- Green IT Strategies in Mobile and Distributed Systems: Sustainable design and management of mobile technologies and data centers
- Life Cycle Assessment (LCA): Application of LCA in IT hardware and software development
- Education and Training for Green IT: Curriculum development, capacity building, and case studies
- Regulatory and Compliance Aspects: Overview of international standards, compliance practices, and green certifications

Prüfung

Verpflichtende Voraussetzung gemäß SPO für die Teilnahme an der Prüfung
Keine

Art der Prüfung
Sonstige Prüfung (soP) gemäß §§ 26, 27 APO

Dauer/Form der Prüfung
Portfolio

Die konkrete Festlegung der abzuleistenden Prüfung erfolgt im Studienplan

Prüfungssprache
Englisch

Voraussetzung für die Vergabe von Leistungspunkten
Keine

Lernergebnisse
Upon successful completion of this module, students will be able to:

- Remember key concepts and terminology related to Green IT, including sustainability goals, environmental impacts, and regulatory frameworks
- Understand the ecological footprint of hardware and software systems and explain how IT contributes to global sustainability challenges
- Apply principles of sustainable software engineering, energy-efficient algorithms, and lifecycle assessments to practical use cases
- Analyze and compare national and regional Green IT strategies and regulatory approaches across Germany, Iceland, and the Czech Republic
- Evaluate the sustainability impact of IT systems and development practices using recognized metrics and standards
- Create innovative, practical solutions to real-world Green IT challenges by working on interdisciplinary, cross-national projects

Literatur
It will be announced in class