Virtuelle Fachhochschule

Modulhandbuch

IT-Sicherheit Bachelor Online

Stand: 18.11.2021

Curriculum in der Fassung von: 2020

BHT Berliner Hochschule für Technik

1 Computerarchitektur und Betriebssysteme

Computer Architecture and Operating Systems

Semester	1
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Dipl.-Inform. Andreas Wilkens, Hochschule Emden/Leer
Lerngebiet	Fachspezifische Grundlagen
Teilnahmevoraussetzungen	keine
Lernergebnisse	Die Studierenden sind in der Lage, … • die grundlegende Von-Neumann-Architektur eines Computers zu verstehen, • die grundlegende Abarbeitung einzelner Befehle auf einem Von-Neumann-Rechner zu verstehen, • die Vorteile erweiterter Komponenten der Rechnerarchitektur (Interrupt-Controller, DMA-Controller, MMU, etc.) zu verstehen, • die grundlegenden Aufgabengebiete eines Betriebssystems zu erinnern, • die Aufgaben und Probleme der Prozessverwaltung eines Betriebssystems zu verstehen, • die Aufgaben und Probleme der Speicherverwaltung eines Betriebssystems zu verstehen, • die Aufgaben und Probleme der Geräteverwaltung eines Betriebssystems zu verstehen, • die Aufgaben und Probleme der Dateiverwaltung eines Betriebssystems zu verstehen.
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme mindestens 66,66%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 131,5 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 4,5 h Prüfung: 120 min
Präsenzart	erfordert physische Anwesenheit

Präsenzinhalte	Klärung von Fragen zu den Modulinhalten; Besprechung von Einsendeaufgaben
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	- Rechnerarchitektur; Andrew S. Tanenbaum & Todd Austin; Pearson Studium; Auflage: 6., aktualisierte; 2014 - Mikroprozessortechnik; Klaus Wüst; Vieweg+Teubner Verlag; Auflage: 4. Aufl. 2011 - Moderne Betriebssysteme; Andrew S. Tanenbaum & Herbert Bos; Pearson Studium; Auflage: 4., aktualisierte (1. Mai 2016) - Modern Operating Systems; Andrew S. Tanenbaum & Herbert Bos; Prentice Hall; Auflage: 4 (4. August 2014) - Grundkurs Betriebssysteme; Peter Mandl; 4., aktualisierte und erweiterte Auflage; Springer Vieweg, 2014 - Betriebssysteme: Grundlagen, Konzepte, Systemprogrammierung; Eduard Glatz; dpunkt.verlag GmbH; Auflage: 3., überarb. u. akt. Aufl. 2015
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
1. Motivation 2. Computerarchitektur • Vom Anwender zur digitalen Schaltung • Prozessoren und ihre Befehle • Weitere Komponenten der Computerarchitektur • Fazit Computerarchitektur 3. Betriebssysteme • Einführung Betriebssysteme • Prozessverwaltung • Speicherverwaltung • Geräteverwaltung • Dateiverwaltung 4. Aufgaben zur Prüfungsvorbereitung

2 Digitaler Selbstschutz

Digital Self-Protection

Semester	1
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Dorina Gumm, Technische Hochschule Lübeck
Lerngebiet	Fachspezifische Grundlagen (IT-Sicherheit)
Teilnahmevoraussetzungen	keine
Lernergebnisse	Die wesentlichen Fragestellungen der Informations- und Datensicherheit sollen verstanden worden sein, damit die Studierenden • Risiken und ihre Relevanz kennen und beschreiben können, • Maßnahmen zur Reduzierung von Sicherheitsrisiken durchführen können, • Werkzeuge bezüglich ihrer Risiken evaluieren können.
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme mindestens 50%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium inkl. Anfertigung der Hausarbeit: ca. 131,5 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Kolloquium: 30 min
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Erörterung wichtiger Fragestellungen in gemeinsamem Austausch, Exploration ausgewählter technischer Szenarien und Schutzmöglichkeiten
Prüfungsform	Hausarbeit mit Kolloquium (30 min)
Literatur	Web-Quellen entsprechend Online-Material Albrecht, Jan Philipp u. a. (2015). Die Datenschutzreform der Europäischen Union. Hrsg. von Jan Philipp Albrecht MdEP. Brüssel.
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
IT-Sicherheit ist ein hochkomplexes Teilthema der Informatik, hat aber inzwischen eine große Relevanz für Anwender bekommen, unabhängig von ihrem technischen und beruflichen Hintergrund. Aus dieser Perspektive ist weniger die (software-)technische Bedrohung für die Absicherung von Systemen relevant, sondern die Frage nach der Sicherheit von Daten, Informationen und Geräten einzelner Personen. Dieses Modul fokussiert daher auf diese Fragestellung und bietet einen Zugang zur IT-Sicherheit, der aus Alltagserfahrungen motiviert ist. Es geht in diesem Modul also um den Umgang mit eigenen Daten und Geräten, den relevanten Problemstellungen bezüglich der Sicherheit und gibt in diesem Rahmen Ausblick auf vertiefende informatische Themen, die im Laufe des Studiums behandelt werden. Damit verfolgt dieses Modul das übergreifende Ziele: für IT-Sicherheit zu sensibilisieren, die Fragestellungen aus dem eigenen Erfahrungskontext heraus zu verstehen und Schutzmaßnahmen aus dieser Perspektive erfahrbar zu machen, um einen sicherheitsbewussten Umgang mit IT und Informationen an den Tag legen zu können. Die Teilnehmer sammeln hier Erfahrungen, um theoretische und methodische Grundlagen weiterer Module besser einordnen zu können. Das Modul besteht aus drei separaten MOOCs, die während des Semesters bearbeitet werden. Die MOOCs decken die folgenden Themen ab: Souveräner Umgang mit Daten und Geräten: • Passwortsicherheit • Endgeräte schützen • Datenaustausch Souveränes Bewegen im Web: • Umgang mit Zugängen • Malvertising • Anonymisierung • Tracken: Spuren im Netz Sicherheit und Kommunikation: • Mailing • Messaging • Eigene und fremde Netze

3 Einführung in die Informatik Introduction to Informatics	
Semester	1
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr.-Ing. Ulrich Klages, Ostfalia Hochschule für angewandte Wissenschaften
Lerngebiet	Fachspezifische Grundlagen (Informatik, Technische Informatik)
Teilnahmevoraussetzungen	Empfehlung: Interesse für mathematische Fragestellungen, grundlegende englische Sprachkompetenz (insbesondere Lesefähigkeit technischer Texte)
Lernergebnisse	Nach dem erfolgreichen Abschluss des Studienmoduls, sind die Studierenden in der Lage, • elementare, auch mathematischen, Strukturen der automatischen Informationsverarbeitung zu erläutern, • gegebene formale Strukturen in atomare Elemente zu analysieren und aufzugliedern, • formale Problemlösungsansätze zu entwickeln, • beispielhafte Modellbildungen und Problemlösungen anzuwenden, • grundlegende Technologien elektronischer Rechenanlagen zu erläutern, • wesentlicher Leistungs- und Komplexitätsmerkmale zu bestimmen, • beispielhafte Datenflüsse und Verarbeitungsinstanzen zu gliedern, • Problemstellungen der Informationsverarbeitung zu formalisieren und zu beschreiben, • formalisierte Problembeschreibungen selbständig zu erstellen, • Standardverfahren zur Arithmetik und Algorithmisierung zu erläutern, • allgemeine Aufgabenstellungen bis hin zu Implementationsansätzen zu strukturieren, • aufgabenspezifische Einflussfaktoren in der Projektarbeit zu bestimmen, • Soll-Ist-Größen der Projektarbeit zu vergleichen und Eingriffsmaßnahmen abzuleiten, • Eigen- und Gruppeneinflüssen auf Arbeitsabläufe zu erkennen, • negative und positive Parameter in der Gruppenarbeit zuzuordnen und zielorientiert auf Gruppenmitglieder Einfluss zu nehmen.

Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme mindestens 50%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Prüfung: 120 min
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Klärung inhaltlicher Fragen, Diskussion von ausgewählten Themen, Klausurvorbereitung. Wegen besseren Lernerfolgs ist die Anwesenheit in der Präsenzphase vorzuziehen.
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Informatik Eine grundlegende Einführung; Broy, Manfred; Bd.1 Programmierung und Rechenstrukturen; 2013 Springer, Berlin Informatik Eine grundlegende Einführung; Broy, Manfred; Bd.2 Systemstrukturen und Theoretische Informatik; 2013 Springer, Berlin Einführung in die Informatik; Gumm, Heinz-Peter u. Sommer, Manfred; 2012 Oldenbourg Funktionale, imperative und objektorientierte Sicht - Algorithmen und Datenstrukturen; Hubwieser, Peter, Mühling, Andreas u. Aiglstorfer, Gerd; 2012; Oldenbourg Informatik: Eine praktische Einführung mit Bash und Python; (weiterführende Ergänzung!);Tobias Häberlein; 2016; de Gruyter; Berlin
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
• Motivation und Geschichte der Informatik • Modellbildung, Graphen, Formalisierung, Abstraktion (auch Petri-Netze, ER-Modell, UML) • Information und Nachricht, Codes • Zahlen und Zahlensysteme, Arithmetik, boolsche Algebra, relationale Algebra • Algorithmen, Software-Entwicklungsprozess • grundlegende Datenstrukturen und Algorithmen (auch Rekursion und Lösungssuchverfahren) • Rechner- und Prozessorarchitekturen (auch v. Neumann-Architektur etc.) • technische Informatik (Maschinenbefehle und Ablaufoptimierung, Ein-/Ausgabeorganisation, Multimedia-Peripherie, Bussysteme, Speichertechnologien) • Leistungsbewertung, Konzepte der Parallelverarbeitung (SIMD/MIMD)

- Betriebssysteme, Basis-/Träger-/Dienstsysteme, Datenbanken, Anwendungssysteme, Client-Server-Architekturen, Cloud-Technologie
- Rechnernetze und Datenkommunikation, Netzstrukturen und -architekturen, Dienste im Internet
- Sicherheit und Datenschutz
- Einbettung der Informatik in die Gesellschaft

4 Grundlagen der Mathematik

Principles of Mathematics

Semester	1
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Rolf Socher, Technische Hochschule Brandenburg
Lerngebiet	Mathematisch-naturwissenschaftliche Grundlagen
Teilnahmevoraussetzungen	keine
Lernergebnisse	Die Studierenden … • sind in der Lage, sicher mit den Grundoperationen des jeweiligen Gebiets umzugehen (Beispiele: Mengenoperationen, logische Junktoren, Matrixoperationen; • können Ausdrücke zwischen verschiedenen Darstellungsformen übersetzen (Beispiele: Mengenausdrücke mit Mengenoperatoren / Mengenausdrücke mit Venn-Diagrammen); • können formale Regeln sicher anwenden, um Terme zu vereinfachen; • können Alltagsproblemstellungen mithilfe der Konzepte des jeweiligen Gebiets modellieren. (Beispiele: Formulierung des Schaltjahrproblems («Wann ist eine Jahreszahl ein Schaltjahr?») mithilfe einer logischen Formel; • haben ein tiefes Verständnis von Begriffen und Zusammenhängen: Sie können Begriffe in unterschiedlichen Kontexten und Anwendungsgebieten erkennen sowie Erkenntnisse miteinander verknüpfen; (Beispiel: Verständnis des Zusammenhangs der Begriffe «lineare Unabhängigkeit», «Erzeugendensystem», «Basis», «Dimension»).
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme mindestens 50%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Prüfung: 120 min
Präsenzart	erfordert physische Anwesenheit

Präsenzinhalte	Kennen lernen, Besprechung der Übungsaufgaben und gemeinsame Bearbeitung weiterer Aufgaben, Klärung inhaltlicher Fragen, Klausurvorbereitung
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Socher, R.: Mathematik für Informatiker. München: Hanser 2011 Papula: Mathematik für Ingenieure und Naturwissenschaftler, Bd. 1 und Bd. 2. Wiesbaden: Springer Vieweg 2014
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
1 Mengen: Zahlenmengen der Mathematik, Mengenoperationen, Mengendiagramme, Potenzmenge, Binomialkoeffizienten, kartesisches Produkt **2 Relationen und Funktionen** **3 Bausteine der Aussagenlogik:** Aussagen und ihre Verknüpfungen, aussagenlogische Formeln **4 Gesetze der Aussagenlogik:** Tautologien und logische Identitäten, Gesetze der Booleschen Algebra, Vereinfachungsregeln, Normalformen **5 Anwendungen der Aussagenlogik:** Mathematische Beweisverfahren, Digitale Schaltnetze **6 Matrizen und Matrixoperationen:** Grundlegende Begriffe, Addition und skalare Multiplikation, die transponierte Matrix, Matrixmultiplikation; Gesetze der Matrixmultiplikation, Einführung in MATLAB/FREEMAT Anwendungen: Münzwanderungen und Bevölkerungswachstum **7 Lineare Gleichungssysteme:** Grundlegende Begriffe, Der Gauß-Algorithmus: Die Spielregeln und die Strategie, die Lösungsmenge linearer Gleichungssysteme, Linearkombinationen und lineare Hülle, Vektorräume, die inverse Matrix, Berechnung der inversen Matrix mit dem Gauß-Algorithmus, die Determinantenfunktion **8 Fehlerkorrigierende Codes (optional):** Codes: Grundlegende Begriffe, die Systeme Z2 und Z2-hoch-n, Generatormatrix und Prüfmatrix, Lineare Codes, Lineare Unabhängigkeit und Basis, Auf der Suche nach einer Basis **9 Analytische Geometrie:** Analytische Geometrie in der Ebene: Winkel, Parameterform der Geradendarstellung; Analytische Geometrie im Raum: Kreuzprodukt, Normalenvektor, Parameterdarstellung und Gleichungsform von Ebenen im Raum

5 Grundlagen der Programmierung 1

Principles of Programming 1

Semester	1
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Agathe Merceron, Beuth Hochschule für Technik Berlin
Lerngebiet	Fachspezifische Grundlagen (Informatik)
Teilnahmevoraussetzungen	keine
Lernergebnisse	Im Modul werden grundlegende Konzepte der objektorientierten Programmierung vermittelt und anhand geeigneter Programmieraufgaben geübt. Nach dem erfolgreichen Abschluss des Studienmoduls, sind die Studierenden in der Lage, • die Syntax der Programmiersprache Java sowie grundlegende Konzepte der objektorientierten Programmierung zu verstehen und zu erklären, • die Dokumentation einiger grundlegenden Klassen der Java Standardbibliothek zu lesen, zu verstehen und diese Klassen in Programmieraufgaben zu nutzen, • kleine bis mittlere Programmieraufgaben zu entwerfen, gut strukturiert zu implementieren, zu testen und zu dokumentieren, • mit anderen Programmierer*innen über Programmieraufgaben verbal und textuell zu kommunizieren, und konstruktiv im Team zusammen zu arbeiten.
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme mindestens 66,66%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 127 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 9 h Prüfung: 120 min
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Gemeinsames Training von Programmierfertigkeiten, welche der Lerneinheiten entsprechen.

Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Arnold, K.; Gosling, J.; Holmes, D.: The JavaTM Programming Language, Fourth Edition, 2005 Eckel, B.: Thinking in Java. Prentice Hall, 4nd Edition 2006, ISBN-13: 978-0131872486 Flanagan, D.: Java in a Nutshell, A Desktop Quick Reference. Cambridge, Köln: O'Reilly, 2005, ISBN 389721332X H. Mössenböck: Sprechen Sie Java?, dpunkt.verlag 2014, ISBN: 978-3-86490-099-0 K. Sierra, B. Bates: Java von Kopf bis Fuß, O'Reilly, 2006 C. Ullenboom: Java ist auch eine Insel. Rheinwerk Computing, ISBN: 978-3-8362-5869-2, 2017 Guido Krüger, Heiko Hansen: Java-Programmierung - Das Handbuch zu Java 8, O'Reilly Verlag Köln, 2014, ISBN 978-3-95561-514-7 Dustin Boswell, Trevor Foucher: The Art of Readable Code. O'Reilly, 2011
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
Titel der Lerneinheiten Die Programmiersprache Java Das erste Java-Programm Attribute, Variablen und Typen Methoden und Konstruktoren Sequenz und Selektion Iteration Paketstrukturen Ausnahmen Vererbung Reihungen Zeichenketten und Aufzählungstypen **Zusatzlerneinheiten (freiwillige Bearbeitung)** Einführung in die Programmierung Programmiersprachen und Programmierung

6 Kommunikation, Führung und Selbstmanagement Communication, Leadership and Self-Management	
Semester	1
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	
Teilnahmevoraussetzungen	
Lernergebnisse	**Thema Führung** • Die Studierenden können **evaluieren,** welche Führungsverhaltensweisen in welchen Szenarien mit hoher Wahrscheinlichkeit zu bestimmten Folgen führen (z.B. Steigerung der Motivation, Innovativität, Gesundheit der Mitarbeitenden) und daraus Handlungsempfehlungen **ableiten**. • Die Studierenden sind in der Lage, führungsbezogene Problemstellungen zu **identifizieren** sowie Führungsverhaltensweisen zu **analysieren** und auf dieser Basis Lösungen zu **entwickeln**. • Die Studierende können das erworbene Wissen und die erlangten Fähigkeiten zum Thema Führung auf eigene Fallbeispiele ihres beruflichen Alltags **übertragen**, um eigenständig Lösungen für führungsbezogene Problemstellungen zu **generieren**. **Thema Selbstmanagement** • Die Studierenden **wissen** um die Bedeutung von Selbstmanagement-Kompetenz als personale Schlüsselressource und **verstehen** deren Funktion im eigenen individuellen privaten und beruflichen Lebenskontext. • Die Studierenden sind in der Lage, anhand eigener Erfahrungen Zusammenhänge zwischen der eigenen Persönlichkeit, Motiven, Werten und Kompetenzen zu **analysieren** und darauf aufbauend zu langfristig tragfähigen Zielen zu **synthetisieren**. • Die Studierenden können verschiedene Ansätze und Instrumente des Selbstmanagements hinsichtlich deren Anwendungskontexte **einordnen** und **bewerten** und darauf aufbauend für sich selbst passgenaue Selbstmanagementstrategien **entwickeln**. **Thema Kommunikation**

	• Die Studierenden **verstehen** die Relevanz der Funktionen von Kommunikation im privaten und beruflichen Kontext und **wissen** um zentrale Erfolgskriterien gelungener Kommunikation. • Die Studierenden sind in der Lage, Präsentations- und Gesprächssituationen zu **analysieren** und auf dieser Basis Gestaltungsansätze und -techniken zur zielführenden Kommunikation zu **entwickeln**. • Die Studierenden können die erlangten Ansätze und Techniken zum Thema Kommunikation auf konkrete Situationen ihres privaten und beruflichen Alltags **übertragen**, die Passung für die jeweiligen Situationen einschätzen und eigenständig Lösungen für diese **generieren**.
Prüfungsvorleistung	Gruppenarbeit via Internet, Präsenzteilnahme mindestens 66,66%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Chat, Einsendeaufgaben u. a.) sowie Präsenzphasen.
Arbeitsaufwand	die ersten beiden Termine sind Pflichtpräsenzen (2x5 Std.)
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Diskussionen, Gruppenarbeiten, Rollenspiele, Präsentationen, praktische Übungen mit Videoanalysen
Prüfungsform	Präsentation mit Rücksprache
Literatur	Day, D. V. (Ed.). (2014). The Oxford handbook of leadership and organizations. Oxford Library of Psychology. Kauffeld, S. (2011). Arbeits-, Organisations-und Personalpsychologie für Bachelor. Berlin: Springer. Nerdinger, F. W., Blickle, G., Schaper, N., & Schaper, N. (2008). Arbeits-und Organisationspsychologie (pp. 445-58). Heidelberg: Springer. Schuler, H., & Kanning, U. P. (Eds.). (2014). Lehrbuch der Personalpsychologie. Hogrefe Verlag. Heath, C. & Heath, D. (2010). Made to stick – Why some ideas survive and others die. New York: Random House. London, M. (2003). Job Feedback. Giving, Seeking, and Using Feedback for Performance Improvement. New Jersey: Lawrence Erlbaum Associates. Luft, J. & Ingham, H. (1969). Johari Window. The Model. (http://richerexperiences.com/wpcontent/uploads/2014/02/Johari-Window.pdf . called: 26.07.2016) Robbins, S.P. & Judge, T.A. (2013). Organizational Behavior. Boston: Pearson.

	Schulz von Thun, F. (1981). Miteinander reden 1. Reinbek: Rowolt. Schulz von Thun, F., Ruppel, J. & Stratmann, R. (2012). Miteinander reden: Kommunikationspsychologie für Führungskräfte. Reinbek: Rowolt. Schulz von Thun, F. (2008). Six Tools for Clear Communication. The Hamburg Approach in English Language. Hamburg: Schulz von Thun Institut für Kommunikation. Shu, S.B. & Carlson, K. A. (2014) When Three Charms but Four Alarms: Identifying the Optimal Number of Claims in Persuasion Settings. Journal of Marketing, 78(1), 127-139.
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
1 Selbstmanagement 1.1 Warum Selbstmanagement? 1.2 Grundlage des Selbstmanagements: Selbsterkenntnis 1.3 Modelle und Ansätze des Selbstmanagements 1.4 Zusätzliche Instrumente, Techniken und Übungen zum Selbstmanagement **2 Kommunikation** 2.2 Begriffsbestimmung und Abgrenzung 2.3 Kommunikationsformen und -mittel 2.4 Kommunikationsmodelle 2.5 Praktische Aspekte der Kommunikation: "Ich und andere" 2.6 Praktische Aspekte der Kommunikation: "Ich an andere" **3 Führung** 3.1 Motivationsförderliche Führung 3.2 Innovationsförderliche Führung und agile Führung 3.3 Gesundheitsförderliche Führung 3.4 Führung 4.0 - Führung in der digitalen Welt 3.5 Führung und Diversity

7 English for Computer Scientists

English for Computer Scientists

Semester	2
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	BA Christof Reinecke, Technische Hochschule Brandenburg
Lerngebiet	Allgemeinwissenschaftliche Ergänzungen (Fremdsprache, Web Science)
Teilnahmevoraussetzungen	Empfehlung: Kenntnisse und Fähigkeiten in Englisch auf mittlerem Niveau (entspricht Stufe B1-B2 GER)
Lernergebnisse	Die Studierenden sind in der Lage … • Englisch als Schlüsselkompetenz zum fachliche Austausch auf virtueller Ebene anzuwenden, • sich die Inhalte unterschiedlicher Medien sprachlich zu erschließen und Adressaten bezogen darzustellen, • den aktuellen Stand der Digitalisierung in den wichtigsten Bereichen darzustellen, • die Dynamik und Komplexität der Digitalisierung und der damit verbundenen gesellschaftlichen, wirtschaftlichen und ethischen Fragestellungen zu verstehen, • Risiken und Chancen der Digitalisierung in einen größeren Kontext einzuordnen und fachübergreifend in Beziehung zu setzen (flexibler Wissenstransfer), • neue Informationen einzuordnen, um das erworbene Wissen eigenverantwortlich zu ergänzen und zu vertiefen (shift from teaching to learning).
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme mindestens 50%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: ca. 6 h Prüfung: 120 Minuten
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform

Literatur	Module.oncampus multimedial aufbereitetes e-learning Material. Das Material wird jährlich bedarfsgerecht aktualisiert, weiterentwickelt oder ersetzt.
weitere Hinweise	Dieses Modul wird auf Englisch angeboten

Studieninhalte
Die Studieninhalte qualifizieren den Absolventen für den Einstieg in das moderne Berufsleben (employability). Englisch dient als Arbeitssprache und das Modul als Forum für das Erarbeiten aller relevanten Themen der Digitalisierung. Studierende entwickeln fachübergreifende Kompetenzen, einen interdisziplinären Ansatz als auch eine kritische Haltung. Aktuelle Themen: The Silicon Valley mindset: exploring Google Space Rush: providing Internet for everyone - Internet of Things Disrupting truth: analyzing Social Media, filter bubbles and echo chambers Narrow AI: discussing current applications Strong AI: exploring machine learning and neural networks Big Data: studying current applications Blockchain Technology: establishing concept and current applications Linux: outlining applications and impact CRISPR: establishing concept and implications Cars turning digital: investigating into autonomous driving, connected mobility Cyberwar: analyzing warfare in a digital age Brave New World?: understanding impact of digitalization on human behaviorSichere agile Organisation und DevOps Security Frameworks

8 Grundlagen der IT-Sicherheit (MI) Principles of IT Security	
Semester	2
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Claus Vielhauer, Technische Hochschule Brandenburg
Lerngebiet	Fachspezifische Grundlagen (IT-Sicherheit)
Teilnahmevoraussetzungen	Empfehlung: Grundlagen der Mathematik, Einführung in die Informatik sowie Theoretische Informatik
Lernergebnisse	Die Studierenden sind in der Lage, ... • wesentliche Zielsetzungen und Begrifflichkeiten aus der IT-Sicherheit (z. B. Sicherheitsaspekte, Risikobegriff, Angreiferszenarien) auf IT-bezogene Sachverhalte anzuwenden; • wesentliche Sicherheitsprobleme in IT- und Medienanwendungen, grundlegende Methoden zu deren Analyse und Modellierung in Sicherheitsmodelle sowie organisatorische und technische Lösungsansätze hierfür wiederzugeben; • Grundlagen zu Sicherheitsmodellen und wesentlichen Sicherheitsstandards zu kennen und zu verstehen; • aktuelle Verfahren zur Erarbeitung und Umsetzung von Sicherheitskonzepten, sowie ausgewählte praktische Sicherheitswerkzeuge anzuwenden; • Sicherheitsaspekte/-anforderungen für spezifische IT-Systeme zu analysieren, technische Schutzmethoden aufzuzeigen, zu differenzieren, zu bewerten und auf diese zu beziehen; • grundlegende Schutzkonzepte auf Basis der behandelten Schutzmethoden zu planen; • künftige Spannungsfelder zwischen gesellschaftlichen Aspekten der IT-Sicherheit, z. B. Persönlichkeitsschutz vs. Überwachung in der digitalen Welt zu erkennen; • die Wirkungsweise von wesentlichen juristischen Rahmenwerken hinsichtlich IT-bezogener Probleme zu verstehen und • organisatorische Konzepte für die Entwicklung von Sicherheitsrichtlinien, Schwachstellenanalyse und forensischen Untersuchungen anzuwenden.
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme mindestens 50%

Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: ca. 6 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Inhaltliche Klärung, Klausurvorbereitung, Besprechung von erweiterten Übungsaufgaben
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Matt Bishop: Computer Security Art and Science. Addison Wesley, 2003 Matt Bishop: Introduction to Computer Security; Addison-Wesley, Boston, ISBN 0-321-24744-2; 2005 Charles P. Pfleger et al.: Security in Computing, Prentice Hall, 4th edition, 2006 Claudia Eckert: IT-Sicherheit, Oldenbourg-Verlag, 2008 Weiterhin finden sich Referenzen zu Publikationen zur tieferen Einarbeitung in den einzelnen Kurseinheiten.
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
1. Einführung und organisatorische Sicherheit • Security versus Safety • Grundlegende Datensicherheitsaspekte und Sicherheitsanforderungen • Sicherheitsrisiken, Sicherheitslücken und bekannte Attacken • Sicherheitspolicies und Modelle • Sicherheitsstandards • Social Engineering 2. Datenschutz und nicht-technische Datensicherheit • EU Datenschutzverordnung, Bundes- und Landesdatenschutzgesetze • Telemediengesetz (TMG), Telekommunikationsgesetz (TKG) und Staatsvertrag für Rundfunk und Telemedien (RStV) • Urheberrecht, Strafgesetzbuch • IT Sicherheitsgesetz 3. Identity Management • Grundlagen der Benutzerauthentifizierung • Wissensbasierte Authentifizierung: Passwörter, One-Time Tokens etc. • Besitzbasierte Authentifizierung: Smartcards & RFID

- Biometrische Authentifizierung
- Multifaktorielle Authentifizierung
- Single-Sign-On Systeme
- Positionsbasierte Authentifizierung

4. Angewandte IT Sicherheit
- Einführung in die IT Forensik
- Einführung in die Mediensicherheit

5. Praktische IT Sicherheit
- Vorgehen bei Sicherheitskonzepten: BSI-Grundschutz
- Ausblick kryptographischer Schutz
- Ausblick Netzsicherheit

9 Grundlagen der Kryptographie

Principles of Cryptography

Semester	2
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Christian Forler, Beuth Hochschule für Technik Berlin
Lerngebiet	Mathematisch-naturwissenschaftliche Grundlagen
Teilnahmevoraussetzungen	Empfehlung: Grundlagen der Mathematik
Lernergebnisse	Nach dem erfolgreichen Abschluss des Studienmoduls, sind die Studierenden in der Lage, • formale Notationen und anzuwenden, • elementare kombinatorische Problemstellungen zu lösen, • grundlegende Algorithmen zur Ganzzahlarithmetik anzuwenden, • den Umgang mit Operationen in Gruppen und Körpern anzuwenden, • die Funktionsweise von elementaren Verfahren der asymmetrischen Kryptographie erklären und anzuwenden, • die mathematische Kernidee von elementaren kryptographischen Verfahren zu erkennen, • sich in weiterführende Gebiete der Kryptographie einzuarbeiten, • grundlegende kryptographische Problemstellungen und Lösungsansätze zu beschreiben.
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme mindestens 50%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Inhaltliche Klärung, Klausurvorbereitung, Besprechung von Übungsaufgaben
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform

Literatur	Einführung in die Kryptographie, Johannes Buchmann, 2016 Springer Spektrum; 6. Auflage; ISBN 3642397743 Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender; Christof Paar und Jan Pelzl; 2016 eXamen.press; ISBN 3662492962
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
In dem Modul werden die mathematischen Grundlagen der Kryptographie vermittelt und geübt. Nach dem erfolgreichen Abschluss sind die Teilnehmenden befähigt kryptographische Bausteine und Verfahren zum Verschlüsseln und Signieren von Daten zu verstehen und deren Sicherheit einzuschätzen. **Teil A: Grundlagen** Kapitel 1: Grundlagen der Aussagelogik Kapitel 2: Ganze Zahlen Kapitel 3: Algorithmen für Ganzzahlen Kapitel 4: Polynome und Permutationen Kapitel 5: Primzahlen Kapitel 6: Diskrete Wahrscheinlichkeiten und Kombinatorik **Teil B: Kongruenzen und Restklassenringe** Kapitel 7: Restklassen Kapitel 8: Gruppen Kapitel 9: Textbook-RSA und DH-Schlüsselaustausch Kapitel 10: Endliche Körper

10 Grundlagen der Programmierung 2

Principles of Programming 2

Semester	2
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Agathe Merceron, Beuth Hochschule für Technik Berlin
Lerngebiet	Fachspezifische Grundlagen (Informatik)
Teilnahmevoraussetzungen	Empfehlung: Grundlagen der Programmierung 1
Lernergebnisse	Im Modul werden fortgeschrittene Konzepte der objektorientierten Programmierung und umfangreichere Klassen der Java Bibliothek, beispielsweise das Collection Framework und graphischen Oberflächen vermittelt und anhand geeigneter Programmieraufgaben geübt. Nach dem erfolgreichen Abschluss des Studienmoduls, sind die Studierenden in der Lage: • fortgeschrittene Konzepte der (objektorientierten) Programmierung wie Interface, Lambda Ausdrücke oder Rekursion in Beispielprogrammen anzuwenden und zu erklären, • mittlere Programmieraufgaben zu entwerfen, zu implementieren, zu testen und zu dokumentieren, • Anwendungen mit graphischen Oberflächen gut zu strukturieren, • Verschiedene Implementierungen von Datenstrukturen zu verwenden, • Java-Bibliotheken zielorientiert zu nutzen, • Konstruktiv mit anderen Programmierer*innen gemeinsam im Team zu arbeiten.
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme mindestens 66,66%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 127 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 9 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Gemeinsames Training von Programmierfertigkeiten, welche den Lerneinheiten entsprechen.

Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Arnold, K.; Gosling, J.; Holmes, D.: The JavaTM Programming Language, Fourth Edition, 2005 Eckel, B.: Thinking in Java. Prentice Hall, 4nd Edition 2006, ISBN-13: 978-0131872486 Flanagan, D.: Java in a Nutshell, A Desktop Quick Reference. Cambridge, Köln: O'Reilly, 2005, ISBN 389721332X H. Mössenböck: Sprechen Sie Java?, dpunkt.verlag 2014, ISBN: 978-3-86490-099-0 K. Sierra, B. Bates: Java von Kopf bis Fuß, O'Reilly, 2006 C. Ullenboom: Java ist auch eine Insel. Rheinwerk Computing, ISBN: 978-3-8362-5869-2, 2017 Guido Krüger, Heiko Hansen: Java-Programmierung - Das Handbuch zu Java 8, O'Reilly Verlag Köln, 2014, ISBN 978-3-95561-514-7 Dustin Boswell, Trevor Foucher: The Art of Readable Code. O'Reilly, 2011 Epple, Anton: JavaFX 8 Grundlagen und fortgeschrittene Techniken, dpunkt.verlag, 2015 Ebbers, Hendrik: Mastering JavaFX controls. McGraw-Hill Education, 2014
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
Titel der Lerneinheiten • Einstieg in Programmieren 2 • Dateien und Datenströme • Abstrakte Klassen und Interfaces • Arraylist • Grundlagen von JavaFX • 2D-Grafik mit JavaFX • Ereignisbehandlung und Binding mit JavaFX • Rekursion • Java und XML • Listen

11 Rechnernetze Grundlagen

Principles of Computer Networks

Semester	2
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Andreas Hanemann, Technische Hochschule Lübeck
Lerngebiet	Fachübergreifende Grundlagen (Informatik)
Teilnahmevoraussetzungen	keine
Lernergebnisse	• Die Studierenden können die Aufgaben, die für die Realisierung von Rechnernetzen zu unterscheiden sind, in das OSI-Modell einordnen. Dadurch können Sie die Vorteile, die die Verwendung eines solchen Schichtenmodells bietet, darlegen. • Die Studierenden können darstellen, auf welche Arten die Verwendung eines gemeinsam genutzten Mediums geregelt werden kann. Dabei sind sie in der Lage, an Randbedingungen (z.B. drahtlose Übertragung) angepasste Verfahren zu bewerten, wobei Kriterien wie Fairness, Stabilität und Durchsatz zu berücksichtigen sind. • Die Studierenden können erklären, wie eine skalierbare weltweite Kommunikation allgemein realisiert werden kann und wie dieses im Internet (d.h. in den entsprechenden Protokollen) implementiert ist. • Die Studierenden können eine Auswahl zwischen Protokollen der Transportschicht treffen, um diese als Basis für Internetanwendungen zu nutzen. Dafür können sie auf Basis der Eigenschaften der Protokolle entscheiden, welche Kriterien für die konkrete Anwendung wichtig sind. • Die Studierenden können bei der Konfiguration von Webanwendungen auf der Basis von HTTP, unterschiedliche Möglichkeiten in Betracht zu ziehen, um damit eine schnelle und zuverlässige Auslieferung der Webinhalte zu den Nutzerinnen und Nutzern zu erreichen.
Prüfungsvorleistung	Einsendeaufgabe
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen

Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Kurose, James F.; Ross, Keith W. (2014): Computernetzwerke. Der Top-Down-Ansatz. 6., aktualisierte Auflage., Pearson Deutschland. Tanenbaum, Andrew S.; Wetherall, David (2012): Computernetzwerke. 5., aktualisierte Aufl., Pearson Deutschland.
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte

Einführung und Netztopologien
- Bedeutung von Kommunikationsnetzen
- Standardisierung und Regulierung

OSI-Referenzmodell
- Grundprinzipien des Modells
- Die Schichten des OSI-Modells
- Transportorientierte Schichten
- Anwendungsorientierte Schichten
- OSI-Modell in der Praxis
- Zwischensysteme

Sicherungsschicht
- Multiplexverfahren
- IEEE Arbeitsgruppe 802
- Ethernet
- Wireless LAN
- Point-to-Point-Protokoll
- Fehlererkennung- und korrektur

Vermittlungsschicht
- Vermittlungsprinzipien
- Adressen der Vermittlungsschicht
- Internet Protocol
- ICMP − Internet Control Message Protocol
- ARP - Address Resolution Protocol
- DHCP - Dynamic Host Configuration Protocol
- Network Address Translation
- Internet Protocol Version 6 (IPv6)

- Migration IPv6/IPv4
- Routing-Verfahren

Transportschicht
- Ports
- UDP − User Datagram Protocol
- TCP - Transmission Control Protocol
- Weitere Transportschichtprotokolle
- Socket API

Anwendungsschicht
- Klassifikation von Anwendungen
- World Wide Web
- E-Mail
- Domain Name System

Geschichtliche Entwicklung

12 Theoretische Informatik

Theoretical Informatics

Semester	2
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. rer.nat. Friedhelm Seutter, Ostfalia Hochschule für angewandte Wissenschaften
Lerngebiet	Fachübergreifende Grundlagen
Teilnahmevoraussetzungen	Empfohlen: Grundlagen der Mathematik, Informatik, Programmierung
Lernergebnisse	Die Studierenden… • kennen grundlegende Modelle und Methoden der Theoretische Informatik und ihre Beziehungen untereinander. • verstehen formale Notationen und die ausgehend von Definitionen durch Sätze ausgedrückten Zusammenhänge und Beziehungen und die verwendeten Konstruktions- und Beweisideen. • verstehen Automatenmodelle und algebraische und generierende Konzepte zur Definition formaler Sprachen. • können die auf formaler Ebenen erworbenen Erkenntnisse auf Anwendungen in der Praxis, unter Berücksichtigung ihrer Beschränkungen, übertragen und anwenden. • können konkrete Probleme analysieren und eine Reduktion und Abstraktion des Problems durchführen, um das unbedingt Notwendige für die Lösung des Problems herauszustellen. • können ein Problem formal darstellen (mittels Modellen und Methoden der theoretischen Informatik), um es zu lösen. • verstehen Beschränkungen und Grenzen der Modelle und Methoden zur algorithmischen Berechnung von Lösungen und können diese in Bezug auf konkrete Anwendungen bewerten und auswählen.
Prüfungsvorleistung	Einsendeaufgabe
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen

Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Zusammenfassung und Wiederholung ausgewählter Abschnitte aus dem Studienmodul, Klärung inhaltlicher Fragen, Besprechung von Übungsaufgaben, Klausurvorberei-tung.
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	- Sipser, M.: Introduction to the Theory of Computation. 3rd Edition. Sengage Learning, 2013. ISBN 13-978-1-133-18781-3 - Hopcroft, John E.; Motwani, Rajeev; Ullman, Jeffrey D.: Introduction to Automata Theory, Languages, and Computation. Third Edition. Boston, Addison-Wesley 2007. ISBN 0-321-47617-4
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
Das Studienmodul gibt eine Einführung in einige grundlegenden Modelle und Methoden der Theoretischen Informatik. Anhand von Automatenmodellen und von diesen analysierbaren formalen Sprachen werden die grundsätzlichen Fähigkeiten und Beschränkungen von Computern und Softwaresystemen untersucht. Dabei stehen insbesondere die Beziehungen zwischen den Automatenmodellen als analysierende Konzepte und den beschreibenden bzw. generierenden Konzepten für formale Sprachen im Vordergrund. Darüber hinaus wird die Frage diskutiert und beantwortet, ob gewisse Probleme überhaupt durch einen Computer oder ein Softwaresystem lösbar sind oder sich einer algorithmischen Berechnung verschließen. Die Studierenden sollen diese Modelle, Methoden und Konzepte kennen lernen und verstehen, sie in ihren fachlichen Kontext einordnen und in konkreten Problemen anwenden können. Die Modelle, Methoden und Konzepte und ihre Beziehungen untereinander werden teils informell erläutert, teils formal definiert bzw. hergeleitet. Für das Studium (insbesondere die Programmierausbildung) und die Praxis (insbesondere die Softwareentwicklung) können diese theoretischen Modelle grundlegende Erkenntnisse und Hinweise zur Lösung diverser Probleme liefern. Computer und Softwaresysteme sind technische Systeme, die mit Hilfe mathematisch-formaler Modelle und Beschreibungen entwickelt und bedient werden. Auch neue Anwendungen sind auf dieser Basis zu konzipieren. Es ist deshalb unerlässlich, abstrakte Modelle und die darauf anzuwendenden Methoden mittels mathematisch-formaler Beschreibungen von Zuständen und Abläufen entwickeln, anpassen und anwenden zu können. Auch diese Kompetenzen sollen mit diesem Studienmodul eingeübt und vertieft werden. **1. Formale Sprachen** 1.1 Alphabete, Wörter und Sprachen 1.2 Zusammenhang mit Programmiersprachen **2. Endliche Automaten**

2.1 Deterministische endliche Automaten
2.2 Nichtdeterministische endliche Automaten
3. Reguläre Sprachen
3.1 Reguläre Sprachen und Operationen
3.2 Reguläre Ausdrücke
3.3 Eigenschaften regulärer Sprachen
4. Kontextfreie Sprachen
4.1 Kontextfreie Grammatiken
4.2 Kellerautomaten
4.3 Eigenschaften kontextfreier Sprachen
5. Turingmaschinen und Berechenbarkeit
5.1 Deterministische Turingmaschinen
5.2 Intuitiver Algorithmusbegriff
5.3 Turing-Berechenbarkeit

6. Entscheidbarkeit
6.1 Entscheidbare Probleme
6.2 Das Halteproblem

13 Algorithmen und Datenstrukturen

Algorithms and Data Structures

Semester	3
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. rer.nat. Friedhelm Seutter, Ostfalia Hochschule für angewandte Wissenschaften
Lerngebiet	Fachübergreifende Grundlagen (Informatik: Algorithmen und Datenstrukturen)
Teilnahmevoraussetzungen	Empfehlung: Grundlagen der Mathematik, Grundlagen der Programmierung 1 + 2
Lernergebnisse	Die Studierenden… • lernen Algorithmen und Datenstrukturen und die darauf angewendeten Techniken zur Verifikation und zur Analyse ihrer Komplexität kennen, • verstehen Such- und Sortieralgorithmen und Speicher- und Zugriffstechniken von bzw. auf Listen, Bäume und Hashtabellen, • verstehen Methoden zur Komplexitätsanalyse von Algorithmen, • können Algorithmen und Datenstrukturen in konkreten Anwendungssystemen zur Lösung einer gestellten Anforderung anwenden und beherrschen, • können Algorithmen verifizieren und bezüglich ihrer Zeit- und Platzkomplexität analysieren, • können Algorithmen und Datenstrukturen weiterentwickeln, um konkrete Probleme zu lösen, • können Algorithmen und Datenstrukturen bezüglich ihrer Zeit- und Platzkomplexität und weiterer Leistungskriterien bewerten und für ihre konkrete Anwendung auswählen.
Prüfungsvorleistung	Einsendeaufgabe
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen

Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Besprechung inhaltlicher Fragen zum Studienmodul Besprechung ausgewählter Übungsaufgaben und gemeinsame Bearbeitung weiterer Beispiele Klärung sonstiger Fragen Klausurvorbereitung
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Corman, Thomas H.; Leiserson, Charles E.; Rivest, Ronald L.: Algorithmen - eine Einführung, 2. Auflage. Oldenbourg Verlag, München 2007. ISBN 978-3-486-58262-8 Baase, Sara; van Geldern, Allen: Computer Algorithms - Introduction to Design and Analysis, 3rd Edition. Addison Wesley Longman Inc., Mass. 2000. ISBN 0-201-612244-5 Schöning, Uwe: Algorithmik. Spektrum Akademischer Verlag, Heidelberg. 2001. ISBN 3-8274-1092-4
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
Das Studienmodul gibt eine Einführung in das Fach Algorithmen und Datenstrukturen. Das Ziel dabei ist einerseits, einige Algorithmen und einige Datenstrukturen kennenzulernen und sie zu verstehen. Im Vordergrund stehen Such- und Sortieralgorithmen und die dynamische Datenstrukturen Listen, Bäume und Hashtabellen. Alle Algorithmen werden in so genanntem Pseudocode dargestellt. Darüber hinaus geht es aber auch um die Analyse von Algo-rithmen. Eine Technik zu deren Verifikation wird kurz eingeführt, die Verfahren zur Bestimmung ihrer Komplexität bzgl. Laufzeit und Speicherplatz werden dagegen tiefergehend diskutiert. Hierfür werden einige Komplexitätsmaße eingeführt und diese auf alle vorgestellten Algorithmen angewendet. Die Studierenden sollen die Algorithmen und Datenstrukturen und die darauf angewandten Analyse-techniken kennen lernen und verstehen, sie in ihren fachlichen Kontext einordnen und in konkreten Problemen anwenden können **Kapitelüberschriften / Überschriften der Lerneinheiten:** 1. Einleitung 1.1 Was ist ein Algorithmus? 1.2 Darstellung von Algorithmen 2. Analyse von Algorithmen 2.1 Verifikation 2.2 Komplexität

2.3 Asymptotische Notation
2.4 Optimalität

3. Rekursion
3.1 Lineare Rekursion
3.2 Divide and Conquer

4. Suchen und Sortieren
4.1 Problemspezifikation
4.2 Sequentielles Suchen
4.3 Binäres Suchen
4.4 Suchen und Optimalität
4.5 Bubble-Sort
4.6 Merge-Sort
4.7 Quick-Sort
4.8 Sortieren und Optimalität
4.9 Sortieren durch Abzählen

5. Dynamische Datenstrukturen
5.1 Abstrakte Datentypen
5.2 Verkettete Listen
5.3 Binäre Bäume
5.4 Binäre Heaps
5.4.1 Konstruktion und Erhalten eines Heaps
5.4.2 Heap-Sort
5.4.3 Prioritäts-Warteschlangen

6. Hashverfahren
6.1 Adresstabelle mit direktem Zugriff
6.2 Hashtabellen
6.3 Hashfunktionen
6.4 Offene Adressierung
6.5 Array Doubling

14 Angewandte Kryptographie

Applied Cryptography

Semester	3
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Patrick Felke, Hochschule Emden/Leer
Lerngebiet	Mathematisch-naturwissenschaftliche Vertiefung
Teilnahmevoraussetzungen	Grundlagen der Kryptographie
Lernergebnisse	In diesem Modul werden die Grundlagen der symmetrischen und asymmetrischen Kryptographie, sowie deren Kryptoanalyse vermittelt und geübt. Nach dem erfolgreichen Abschluss sind die Teilnehmer befähigt kryptographische Verfahren zu verstehen, deren Wertigkeit einzuschätzen und geeignete Verfahren für bestimmte Anwendungszwecke auszuwählen. Darüber hinaus kennen die Teilnehmer typische Algorithmen zur Implementation von Kryptosystemen und deren kryptoanalytischen Fallstricke bei der Umsetzung. Nach Abschluss des Moduls sind die Studierenden in der Lage • Algorithmen zur symmetrischen und asymmetrischen Verschlüsselung zu verstehen und anzuwenden, • Sicherheitsmodelle zu verstehen und zur Einschätzung der kryptologischen Wertigkeit von asymmetrischen und symmetrischen Verfahren anzuwenden, • moderate Fragestellungen zur Kryptologie selbstständig zu verstehen bzw. zu lösen, • den kryptoanalytischen Kern von kryptologischen Fragestellungen zu extrahieren und deren Einfluss auf die Umsetzung zu verstehen, • geeignete Sicherheitsparameter für den jeweiligen praktischen Einsatz auszuwählen, • kryptographische Verfahren und Protokolle zu implementieren und Fallstricke bei der Umsetzung zu erkennen, • sich in weiterführende Gebiete der Kryptologie einzuarbeiten.
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme 50%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen

Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Inhaltliche Klärung, Klausurvorbereitung, Besprechung von Übungsaufgaben
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender; Christof Paar und Jan Pelzl; 2016 eXamen.press; ISBN 3662492962 Cryptography, Theory and Practice; D. Stinson; Chapman and Hall/CRC Press 2005; ISBN 9781584885085 Post-Quantum Cryptography; D. Bernstein, J. Buchmann, E. Dahmen 2008; Springer ISBN 978-3-540-88701-0 Einführung in die Kryptographie, Johannes Buchmann, 2016 Springer Spektrum; 6. Auflage; ISBN 3642397743
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
In dem Modul werden die wesentlichen Grundlagen der angewandten Kryptographie vermittelt und geübt. Die symmetrische und asymmetrische Kryptographie einschließlich der Grundlagen von Hashfunktionen werden vermittelt und geübt. Die mathematischen, algorithmischen und kryptoanalytischen Aspekte werden vorgestellt und diskutiert. Nach dem erfolgreichen Abschluss sind die Teilnehmenden befähigt kryptographische Bausteine und Verfahren zum Verschlüsseln und Signieren von Daten zu verstehen, deren Sicherheit einzuschätzen und diese umzusetzen bzw. einzusetzen. Ferner sind sie in der Lage einzelne Angriffe auf Kryptosysteme zu verstehen und diese ggf. umzusetzen. **Lehreinheiten** 1. Einführung in Kryptographie 2. Symmetrische Kryptographie • Stromchiffren • Blockchiffren • Zufallsgeneratoren/Sequenzen • Kryptoanalyse 3. Asymmetrische Kryptographie • Public - Key Kryptosysteme • Kryptoanalyse

4. Authentizierung

- Hashfunktionen
- Digitale Signaturen
- Message Authentication Codes (MACs)
- Kryptoanalyse

5. Schlüsselverteilung/-erzeugung
- Symmetrische schlüsselverteilung
- Public Key Infrastructure (PKI)
- Zertifikate

6. Ausblick Post-Quantum Kryptographie

15 Datenbanken

Database Management Systems

Semester	3
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. habil. Torsten Sander, Ostfalia Hochschule für angewandte Wissenschaften
Lerngebiet	Fachübergreifende Grundlagen (Informatik , Datenbanken, Datenbankprogrammierung)
Teilnahmevoraussetzungen	Empfehlung: Grundlagen der Mathematik, Einführung in die Informatik
Lernergebnisse	Die Studierenden… • lernen Datenbankkonzepte und –modelle, relationale Algebra und die Vorgehensweisen bei der Modiellierung kennen und können diese in ihren fachlichen Kontext einordnen und anhand von einigen Miniwelten anwenden. • lernen die reale Welt (z.B. Hochschule, Produktionsbetrieb, etc.) kennen. • verstehen Miniwelten (Ausschnitte aus der realen Welt) und können diese einordnen. • können Miniwelten modellieren und auf gängigen Datenbanksystemen umsetzen. • Kennen Aufgaben und Komponenten eines Datenbanksystems. • verstehen die Funktionsweise von Datenbanksystemen. • können die deskriptive Datenbanksprache SQL zur Datendefinition, -manipulation, -abfrage, Rechteverwaltung und Transaktionssteuerung anwenden. • können Datenmodelle und Datenbanksysteme beurteilen.
Prüfungsvorleistung	Einsendeaufgabe
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen

Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Klärung inhaltlicher Fragen, Diskussion von ausgewählten Themen, Klausurvorbereitung.
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	R. Elmasri, S. B. Navathe: Grundlagen von Datenbanksystemen, Addison-Wesley A. Heuer, G. Saake: Datenbanken, International Thomson Publishing
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
1. Grundlagen 2. Entity-Relationship-Modellierung 3. Relationenmodell 4. Vom ER-Modell zum Relationenmodell 5. Normalformen 6. Relationenalgebra 7. Structured Query Language 8. Performanz 9. Schutz der Daten 10. Transaktionsverwaltung 11. Anwendungsentwicklung

16 Internet-Technologie Internet Technology	
Semester	3
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. rer. nat. Jörg Thomaschewski, Hochschule Emden/Leer
Lerngebiet	Fachübergreifende Grundlagen (Informatik)
Teilnahmevoraussetzungen	Empfehlung: Grundlagen der Programmierung 1
Lernergebnisse	Nach dem erfolgreichen Abschluss des Studienmoduls, erreichen die Studierenden folgende Lernergebnisse. Die Studierenden…. • lernen und vergleichen unterschiedliche Programmiersprachen bezüglich ihrer Semantik und Syntaktik. • erstellen und evaluieren Reguläre Ausdrücke zur Absicherung der an den Webserver gesendeten Daten. • verstehen unterschiedliche Programmierkonzepte. • erstellen eine kleine Website, die im Verlauf des Semesters stetig an Umfang zunimmt. Die Aufgabe fördert die Design- und Realisierungskompetenzen. • erstellen eine kleine Website, die im Verlauf des Semesters stetig an Umfang zunimmt. Die Aufgabe umfasst HTML, CSS, JavaScript, JSON, Ajax, HTTP-Analyse, Webserverkonfiguration, PHP-Grundlagen und Reguläre Ausdrücke. • evaluieren einfache Beispiele der Frondend-Entwicklung bezüglich der eingesetzten Programmiersprachen und Methoden. • verstehen die Zusammenhänge zwischen der Serverkonfiguration, dem Protokoll HTTP und der Server Programmierung und der zugehörigen Absicherung von Webservern bzw. der darauf laufenden Scriptsprachen. Fachübergreifend verstehen Sie damit das Zusammenspiel zwischen Frondend-Entwicklung, Backend-Entwicklung, Systemadministratoren und IT-Sicherheitsspezialisten. • verstehen die Datenübertragung mittels HTTP zwischen Client-Anfragen und den Antworten der Webserver • erstellen eine kleine Website, die im Verlauf des Semesters stetig an Umfang zunimmt. Hierdurch wenden die Studierenden kontinuierlich die Entwicklungsumgebungen an und eignen sich Maßnahmen zur kontinuierlichen Selbstorganisation an.

Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme mindestens 50%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Vorführen komplexerer Beispiel; Klärung inhaltlicher Fragen; Vorstellung der Lösungskonzepte zu den Einsendeaufgaben
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Bei den aktuellen Programmierthemen sind viele Internetquelle im Modul verlinkt, z.B. w3c.org, apache.org
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
In diesem wird Modul eingeübt, mit welchen Techniken eine Internetanwendung erstellt wird: Erstellung der HTML-Seite (inkl. CSS, JavaScript) mit Datenaustausch (z.B. JSON, XML, Ajax, HTTP) und der Konfiguration des Webservers bis zur Programmierung mit PHP und dessen Absicherung mittels Regulärer Ausdrücke. 1. Die Geschichte des Internets 2. HTML 3. DOM 4. CSS 5. JavaScript 6. XML 7. JSON, RESTful, Ajax 8. HTTP 9. Webserver 10. Grundlagen der PHP-Programmierung 11. Reguläre Ausdrücke Anhang: Einrichten der Arbeitsumgebung

17 Netzwerksicherheit Network Security	
Semester	3
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Andreas Hanemann, Technische Hochschule Lübeck
Lerngebiet	Fachspezifische Grundlagen (Informatik)
Teilnahmevoraussetzungen	keine
Lernergebnisse	• Die Studierenden können die Relevanz von aktuellen und zukünftigen Angriffsszenarien auf Kommunikationsnetze einschätzen. Sie können außerdem vorgestellte Tools anwenden, um selbstständig einfache Sicherheitsuntersuchungen durchzuführen. • Die Studierenden können eine angemessene Lösung zum Schutz vor Angriffen aus dem Internet ausarbeiten. Angemessen bedeutet hier, dass diese Lösung eine geeignete Abwägung zwischen dem Nutzen durch die Abwehr möglicher Gefahren und dem Aufwand für die Durchführung der Schutzmaßnahmen darstellt. • Die Studierenden können für die Kommunikation über nicht vertrauenswürdige Netze eine existierende Lösung hinsichtlich der Sicherheitsaspekte (inklusive von Verfügbarkeitsaspekten) bewerten und alternative Lösungen unter Verwendung von bekannten Protokollen entwerfen.
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme mindestens 50%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit

Präsenzinhalte	In der ersten Präsenz werden verschiedene Sicherheitsprotokolle (insbesondere IPsec und SSL/TLS) untersucht. In der zweiten Präsenz wird eine Aufgabensammlung zur Klausurvorbereitung besprochen.
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Wolfgang Böhmer, "VPN - Virtual Private Networks", 2. Auflage, Hanser, 2005 James Kurose, Keith Ross, "Computernetzwerke", 6. Auflage, Pearson Studium, 2014 Claudia Eckert, "IT-Sicherheit", 9. Auflage, Oldenbourg Verlag, 2014
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
• LE 1: Einführung • LE 2: Angriffe auf Kommunikationsnetze • LE 3: Schutz von Kommunikationsnetzen • LE 4: Sichere Kommunikation

18 Sicherheitsmanagement

Security Governance

Semester	3
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Modulverantwortliche(r)	Prof. Dr. Ivo Keller, Technische Hochschule Brandenburg
Lerngebiet	Fachspezifische Grundlagen
Teilnahmevoraussetzungen	Empfehlung: Grundlagen der IT-Sicherheit
Lernergebnisse	Die Studierenden haben nach Abschluss des Moduls verstanden, dass Sicherheitsanforderungen eine ganzheitliche Sichtweise bedingen und nach Effektivitäts- und Effizienzkriterien umgesetzt werden. Die Studierenden sind final in der Lage, • die tragenden Geschäftsprozesse zu analysieren und daraus die Unternehmenswerte abzuleiten, • eine IT-Infrastruktur und den Netzwerkverkehr zu analysieren, • eine Angreifer-, bzw. Bedrohungsmodellierung durchzuführen, • das Risiko für Unternehmens-, Software-Entwicklungs- und ggf. auch für Software-Prozesse einzuschätzen, zu priorisieren und effektive und effiziente Maßnahmen vorzuschlagen, • die Verhältnismäßigkeit der Gegenmaßnahmen zu erklären. • Sie kennen und können anwenden: • organisatorische Sicherheits-Maßnahmen, • BSI-Standards und ISO-Normen, wie die 27000er Familie, • kryptographische Verfahren, das Identitäts- und Zugriffsmanagement (IAM) sowie die Public Key Infrastruktur (PKI).
Prüfungsvorleistung	keine
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 133 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 3 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	inhaltliche Klärung, Vorstellung des Lösungskonzepts des Projekts
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform

Literatur	Sachar Paulus: „Basiswissen Sichere Software“, dpunkt.verlag, 2011 Heinrich Kersten: „IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls“, 2016 (978-3658146931) Müller, Klaus-Rainer: „IT-Sicherheit mit System“, 5. Aufl., Springer Vieweg, 2014 Adam Shostack: „Threat Modeling: Designing for security“, Wiley, 2014 Michael Howard: „Sichere Software programmieren“, Microsoft Press, 2002 Microsoft Security Development Lifecycle (SDL), 2012, https://msdn.microsoft.com/en-us/library/windows/desktop/cc307748.aspx Microsoft: „The STRIDE Threat Model“, 2005 http://msdn.microsoft.com/library/ms954176.aspx Claudia Eckert: „IT-Sicherheit. Konzepte - Verfahren – Protokolle“, Oldenbourg, 2009, http://www.worldcat.org/oclc/463676855
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
1. Ganzheitliches Sicherheitsmanagement 2. Software-Qualität und Sicherheits-Anforderungen 3. Compliance und Normen 4. Bedrohungsmodellierung im Unternehmen, Software Development Lifecycle und Code 5. Risikomanagement 6. Sichere agile Organisation und DevOps 7. Security Frameworks

19 Einführung in wissenschaftliche Projektarbeit

Introduction to Scientific Project Work

Semester	4
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Friedhelm Mündemann, Technische Hochschule Brandenburg
Lerngebiet	Allgemeinwissenschaftliche Ergänzungen (Soft Skills , Wissenschaftliches Arbeiten)
Teilnahmevoraussetzungen	Empfehlung: Kommunikation, Führung und Selbstmanagement
Lernergebnisse	Nach dem erfolgreichen Abschluss des Studienmoduls, sind die Studierenden in der Lage, • eine Dokumentation der Projektphase im Studium zu erstellen. • die formalen Ansprüche an wissenschaftliches Arbeiten zu benennen. • Quellen zu bewerten und rechtssicher zu zitieren. • die Regeln wissenschaftlichen Arbeitens zu befolgen. • folgerichtige Argumentations- und Gedankenmuster anzulegen und zu verwenden. • ein (auch fachübergreifendes) Thema nach wissenschaftlichen Methoden zu planen, experimentell umzusetzen, zu bewerten und darzustellen sowie Arbeitsergebnisse nach wissenschaftlichen Standards zu präsentieren.
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme mindestens 50%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium inkl. Anfertigung der Hausarbeit: ca. 131,5 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Kolloquium: 30 Minuten
Präsenzart	In Online-Konferenz möglich
Präsenzinhalte	Seminarvorträge üben Gliederungen üben Korrektur der Recherche und des Referates
Prüfungsform	Hausarbeit mit Kolloquium (30 min)

Literatur	Frank Vahid: How to Be a Good Graduate Student. Wanda Pratt: Graduate School Survival Guide Dianne O'Leary: Graduate Study in the Computer and Mathematical Sciences: A Survival Manual David Chapman: How to do Research At the MIT AI Lab John W. Chinneck: How to Organize your Thesis, 1999 Alan Bundy, Ben du Boulay, Jim Howe, Gordon Plotkin: The Researcher's Bible Phil Agre: Networking on the Network Knuth, Larrabee, Roberts: Mathematical Writing, the Mathematical association of America DIN 1505, Teil 2,3 Uhlemann Jürgen; Verfassung eines wissenschaftlichen Textes (Versuchsprotokoll, Veröffentlichung u. ä.); Institut für Aufbau- und Verbindungstechnik, TU Dresden 2004; im Web
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
Ziel dieses Moduls ist das Heranführen der Teilnehmerinnen und Teilnehmer an das allgemeine wissenschaftliche Arbeiten mit besonderen Hinweisen zu interdisziplinären Vorgehensweisen im Bereich der Medieninformatik. Dabei werden die zentralen Teilbereiche des Prozesses vorge-stellt und erläutert sowie an Beispielen eingeübt: • Wie suche und nutze ich Literatur und andere Quellen? • Wie sieht eine gute Analyse und Konzeption aus? • Wie gestalte ich die Dokumentation und wie präsentiere ich meine Ergebnisse? Kap. 0: Modulaufbau, Inhalte und Einführung Kap. 1: Wissenschaftliche Arbeiten Kap. 2: Arbeitstechniken Kap. 3: Wissenschaftliches Schreiben und Beurteilen Kap. 4: Wissenschaftliches Präsentieren Kap. 5: Projekte und Projektarbeit

20 Entwicklung sicherer Softwaresysteme Development of Safe Software Systems	
Semester	4
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Dr.-Ing. Martin Schafföner, Technische Hochschule Brandenburg
Lerngebiet	Fachspezifische Grundlagen
Teilnahmevoraussetzungen	keine
Lernergebnisse	Die Studierenden können die für die Entwicklung sicherer Softwaresysteme notwendigen Tätigkeiten im gesamten Softwarelebenszyklus sinnvoll auswählen und durchführen. Sie kennen relevante Best Practices (z.B. Microsofts Secure Development Lifecycle, Open Web Application Security Project), Normen (z.B. ISO 27000-Reihe) und regulatorische Werke (z.B. Medizinproduktegesetz). Studierende können Anforderungen bzgl. der Softwaresicherheit mittels Schutzbedarfs- und Risikoanalysen erheben und dokumentieren. Sie können Entwurfsentscheidungen zur Umsetzung der Anforderungen bewerten und auswählen, z.B. durch Anwendung bewährter Sicherheits-Entwurfs- und Architekturmuster, insbsd. für mobile und verteilte Systeme sowie für mandantenfähige Cloud-Anwendungen. Studierende kennen typische Fehlerquellen bei der Implementierung sicherer Software. Sie können mittels Aspektorientierter Programmierung eine sinnvolle Trennung fachlicher und sicherheitsspezifischer Aufgaben, z.B. Authentisierung und Autorisierung, sicheres Logging oder Auditierung, umsetzen. Studierende können besondere Testmethoden und Qualitätssicherungsverfahren zur Überprüfung von Sicherheitsaspekten auf allen Ebenen der Testhierarchie anwenden. Sie können relevante Best Practices für den Betrieb sicherer Software benennen, insbsd. bzgl. Virtualisierung von Hardware, Netzwerksicherheit und Patchmanagement.
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme mindestens 50%

Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Inhaltliche Klärung, Vorstellung der Lösungskonzepte von ausgewählten Aufgaben.
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Sachar Paulus: „Basiswissen Sichere Software“, dpunkt.verlag, 2011 Fred Long: „Java Coding Guidelines“, Software Engineering Institute, 2013 Michael Howard: „Sichere Software programmieren“, Microsoft Press, 2002 Bolt William: „Engineering Secure Software“, 2016 Microsoft Security Development Lifecycle (SDL), 2012, https://msdn.microsoft.com/en-us/library/windows/desktop/cc307748.aspx Adam Shostack: „Threat Modeling: Designing for security“, Wiley, 2014 Ross Anderson: „Security Engineering: A Guide to Building Dependable Distributed Systems“, Wiley, 2008 Claudia Eckert: „IT-Sicherheit. Konzepte - Verfahren – Protokolle“, Oldenbourg, 2009, http://www.worldcat.org/oclc/463676855
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
1. Einbettung und Ziele der Entwicklung sicherer Softwaresysteme 2. Überblick: Secure Software Development Lifecyle 3. Bedrohungsanalyse 4. Sicherheits-Antimuster, Analyse von Bestandscode 5. Architektur- und Entwurfsprinzipien 6. Best Practices für sichere Softwareentwicklung mit ausgewählten Programmiersprachen 7. Identitäts- und Zugriffsverwaltung 8. Aspect-Oriented Programming am Beispiel: Authentisierung/Autorisierung, Audit-Logs 9. Testen von Sicherheitsanforderungen 10. Sicherheits-Metriken für kontinuierliches Feedback im Entwicklungsprozess 11. Nationale und internationale Normen und andere Regelungswerke 12. Betriebsaspekte für sichere Software: Virtualisierung, Patch-Management

21 Ethik in der IT-Sicherheit

Ethics of IT Security

Semester	4
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Christian Forler, Beuth Hochschule für Technik Berlin
Lerngebiet	Fachspezifische Grundlagen
Teilnahmevoraussetzungen	Empfehlung: Grundlagen der IT-Sicherheit, Einführung in die Informatik
Lernergebnisse	Nach Abschluss des Moduls ... • kennen die Studierenden die Nahtstelle von disziplinären und interdisziplinären Zusammenhänge. • kennen die Studierenden den Unterschied zwischen legalen und legitimen Handlungen. • verstehen die Studierenden die Wechselwirkungen von technologischen Innovationen und gesellschaftlichen Innovationen; insb. die ethische Dimension wissenschaftlichen und praktischen Handelns. • können die Studierenden technischen Handlungen auf soziale, juristisch-normative und gesellschaftliche Dimensionen anwenden, gewichten und beurteilen. • können die Studierenden Implikationen von Maßnahmen, Vorgaben und Dienstanweisungen und von Gewohnheiten auf ethische, normative und juristische Wechselwirkungen hin analysieren. Zudem werden sie befähigt, eine Technikfolgenabschätzung von Handlungen und Innovationen zu treffen. • wissen die Studierene um Sie den Unterschied zwischen deskriptiven und normativen Methoden und Handlungen und wissen, nach welchen Mechanismen sich normative Methoden aufbauen. • verstehen die Studierenden Dimension, Bedeutung und Reichweite von normativen Methoden und Normen. Sie verstehen den Unterschied zwischen juristischen Normen und ethischen Normen. • lernen die Studierenden die Reflexion des eigenen Verhaltens; Umgang mit juristischen Grauzonen und Folgenabschätzung des eigenen und des Handelns Dritter.

Prüfungsvorleistung	Einsendeaufgabe
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium inkl. Anfertigung der Hausarbeit: ca. 131,5 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Kolloquium: 30 Minuten
Präsenzart	erfordert physische Anwesenheit
Prüfungsform	Hausarbeit mit Kolloquium (30 min)
Literatur	Datenschutz Grundverordnung in der jeweils aktuellen Fassung Kurt Lewin: Die psychologische Situation bei Lohn und Strafe 1932 Paul Watzlawick, John H. Weakland, Richard Fisch: Change 1974 Die Hackerethik des Chaos Computer Clubs Kim Zetter: Countdown to Zero Day 2014
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
1. Einführung 2. Datensicherung (Festplatten, Mails etc.) 3. Tracking im Web 4. Heimnetz (Heimrouter, Virenscanner) 5. Medien-Absicherung

22 Hardware-Sicherheit

Hardware Security

Semester	4
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Oliver Stecklina, Technische Hochschule Lübeck
Lerngebiet	Fachspezifische Grundlagen (Informatik)
Teilnahmevoraussetzungen	Empfehlung: Grundlagen Programmierung 1 + 2, Grundlagen der Kryptographie, Computerarchitektur und Betriebssysteme, Rechnernetze Grundlagen, Grundlagen IT-Sicherheit
Lernergebnisse	Nach Abschluss des Moduls sind die Studierenden in der Lage • die Effiktivität und Effizienz von hardware-basierten IT-Sicherheitslösungen abzuschätzen, • Anforderungen zur sicheren Bescheinigung von Fähigkeiten von System-Modulen zu formulieren, • anwendungsspezifische Lösungen auf der Grundlage von technischen Methoden und Verfahren der Hardware-basierten Sicherheit zu gestalten, • Methoden und Verfahren physischer Angriffe zu benennen, • Umsetzung Hardware-basierter Krypto-Funktionen und Zufallszahlengeneratoren zu beschreiben, • Lösungen für eine manipulationssichere Hardware zu benennen, • Krypto-Funktionen hinsichtlich ihrer technischen Eignung in Klein- und Kleinstsystemen zu untersuchen und zu unterscheiden, • Bedeutung und Gefahren von Klein- und Kleinstsystemen für die moderne Gesellschaft einzuordnen und zu erläutern.
Prüfungsvorleistung	Einsendeaufgabe
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium inkl. Anfertigung der Hausarbeit: ca. 131,5 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Kolloquium: 30 Minuten
Präsenzart	erfordert physische Anwesenheit

Prüfungsform	Hausarbeit mit Kolloquium (30 min)
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
In diesem Modul werden Kenntnisse zur technischen Umsetzung von Mechanismen und Algorithmen der IT-Sicherheit vermittelt. Der Schwerpunkt des Moduls liegt auf den Hardware-basierten Problemstellungen und Lösungen in Klein- und Kleinstsystemen. Die Studierenden können im Anschluss Fragenstellungen zur Hardware-basierten Umsetzung von Sicherheitsfunktionen hinsichtlich ihrer anwendungsspezifischen Eignung prüfen bzw. geeignete Lösungsansätze zusammenstellen und deren Effektivität und Effizienz abschätzen. **Lehreinheiten** 1. Einführung in Klein- und Kleinstsysteme 2. Methoden und Verfahren physischer Angriffe • Hardware-Hacking • Seitenkanal-Angriffe 3. Vertrauenswürdige System-Module • Hardware-basierte Krypto-Funktionen • Sichere Zufallszahlen • Remote Attestation 4. Manipulationssichere Hardware • Hardware-Verschlüsselung • Physical Unclonable Functions • Tamper-Resistenz

23 IT-Forensik IT Forensics	
Semester	4
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. rer. nat. Reiner Creutzburg, Technische Hochschule Brandenburg
Lerngebiet	Fachspezifische Grundlagen (Informatik)
Teilnahmevoraussetzungen	Empfehlung: Computerarchitektur und Betriebssysteme, Rechnernetze Grundlagen, Grundlagen der IT-Sicherheit
Lernergebnisse	Nach dem erfolgreichen Abschluss des Studienmoduls, sind die Studierenden in der Lage, • ein grundlegendes Verständnis in Bezug auf mögliche Angriffe auf IT-Systeme und geeignete Gegenmaßnahmen zu entwickeln, • mögliche Schwachstellen und Bedrohungen für ein IT-System zu identifizieren, • Effektivität und Effizienz von IT-Sicherheitslösungen abzuschätzen, • Hash-Verfahren und Write-Blocker einzusetzen, • computerforensische Spuren zu erkennen, zu sichern und auszuwerten, • forensische Hard- und Software-Tools anzuwenden, • Merkmale gerichtfester, forensischer Gutachten einzuhalten und exemplarisch anzuwenden.
Prüfungsvorleistung	Einsendeaufgabe
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 133 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 3 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Inhaltliche Klärung; Vorstellung Lösungskonzept des Projekts
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform

Literatur	Geschonneck A.: Computer Forensik: Systemeinbrüche erkennen, ermitteln, aufklären. Dpunkt.GmbH. ISBN 3-89864-253-4. 2008 Farmer D..: Forensic discovery. Addison-Wesley. ISBN 0-201-63497-X. 2004 Carrier B.: File System Forensic Analysis. Addison Wesley Professional. ISBN 0-32-126817-2. 2005 Kent K., Chevalier S., Grance T., Dang H.: Guide to Integrating Forensic Techniques into Incident Response - NIST Special Publication 800-86. 2006 Chang-Tsun Li (Ed.): Multimedia Forensics and Security. Information Science Reference. ISBN 978-1-59904-869-7. 2009 Nelson B., Phillips A., Steuart Chr.: Guide to Computer Forensics and Investigations. Course Technolpogy ISBN 1-4354-9883-6. 2010
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
Die Studierenden können einen Überblick zur Bedeutung und zu Methoden und Tools der IT-Forensik geben und erste Erfahrungen anwenden. Sie sind in der Lage Risiken einzuschätzen, Bedrohungen abzuwägen und Maßnahmen zur Sicherung von Rechnernetzen und –anwendungen zu ergreifen. Nachdem Studierende das Modul erfolgreich absolviert haben, können sie Sicherheitsprobleme in existierenden IT-Anwendungen benennen und für künftige abschätzen. Sie können Multimedia-spezifische Umsetzungen von Sicherheitsprotokollen für Bild, Video und Audio sowie weitere Mediendaten anwenden. Die Studierenden sind in der Lage, Methodik bei Entwurf und Anwendung von Sicherheitssystemen und -protokollen für Mediendaten einzusetzen. Die Studenten erwerben praktische Fähigkeiten beim Ethical Hacking durch das Lösen von Aufgaben im Hacking-Lab (www.hacking-lab.com). **Lehreinheiten** 1. Motivation und Einleitung 2. Ablauf von Angriffen 3. Digitale Spuren finden und deuten 4. Vorgehensmodelle & grundlegende Strategien 5. Einsatz Computerforensischer Werkzeuge 6. Beispiel praktische IT Forensik 7. Einführung und Vertiefung in die Medienforensik 8. Case Studies

9. Juristische Aspekte

24 Softwaretechnik Software Engineering	
Semester	4
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Stefan Edlich, Beuth Hochschule für Technik Berlin
Lerngebiet	Fachübergreifende Grundlagen (Informatik)
Teilnahmevoraussetzungen	Empfehlung: Sichere Anwendung von Hochsprachen wie Java, C++
Lernergebnisse	Nach dem erfolgreichen Abschluss des Studienmoduls, sind die Studierenden in der Lage: • softwaretechnische Kenntnisse in Projekte und in die Projektarbeit zu übertragen und anzuwenden, • Anforderungsermittlung und Verwaltung eigenständig durchzuführen, • informationstechnische Sachverhalte grafisch darzustellen, • tragfähige IT-Architekturen zu entwerfen und zu gestalten, • zu entscheiden und abzuwägen, wann welches (bestimmtes) Vorgehensmodell besser geeignet ist als ein anderes, • Requirements Engineering im Rahmen der Projektarbeit einzusetzen und zu erklären, • die Hauptprobleme der Softwareentwicklung durch Analyse und Berücksichtigung der wichtigsten Anforderungsmerkmale zu identifizieren, • im Rahmen der Analyse - Pflichten- und Lastenheft, Use-Cases und Requirements einzuordnen und zu erstellen, • den geeigneten Einsatz von UML zu beurteilen und UML praktisch an einem eigenen Projekt anzuwenden und die kritische Nutzung dieser Industriesprache zu berücksichtigen, • zu beurteilen, welche UML-Diagramme in welcher Reihenfolge anzuwenden sind, um ein Modellierungsziel zu erreichen, • die Bedeutung der Architektur im Designprozess zu erklären und diese auf Projekte anzuwenden und zu begründen, • Werkzeuge für das systematische und objektorientiere Testen einzusetzen und selber Tests zu entwerfen, • die Möglichkeiten und Grenzen des Refactoring zu erklären und unter Eclipse oder einer anderen DIE anzuwenden, u.a. durch identifizieren von Bad Code Smell,

	• die Funktionen des Buildmanagements mit ANT praktisch einzusetzen, • die Konzepte des Versions- und Fehlermanagements zu erklären und die bekanntesten Systeme praxisnah zu verwenden, • die Bedeutung von Metriken als Qualitätsmaß praktisch zu beurteilen und Basismetriken zu berechnen, • Codemetriken und deren Werkzeuge zu gebrauchen (bspw. Architekturmetriken und deren Visualisierung), • das Entwurfsmuster Dependency Injection unter Verwendung unterschiedlicher Frameworks in Projekten zu nutzen.
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme mindestens 33,33%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 127 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 9 h Prüfung: 120 Minuten
Präsenzart	In Online-Konferenz möglich
Präsenzinhalte	A) Praxisübungen mit UML. Durchführung eines konkreten Fallbeispieles B) Praxisübungen in den Bereichen Qualitätssiche-rung (Testen) C) Praxisübung in den Bereichen Buildmanagement, Versionsmanagement, etc.
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Balzert, Lehrbuch der Softwaretechnik Oesterreich, Analyse und Design mit UML 2.5 Christ Rupp, Requirements Engineering Balzert, Lehrbuch der Objektmodellierung Ian Sommerville, Softwaretechnik (Global Edition) Jeckle, UML 2 glasklar
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
01 Einführung in die Softwaretechnik 02 Vorgehensmodelle / agile Modelle 03 Requirements Engineering 04 Analyse 05 Unified Modeling Language 06 Objektorientiertes Design 07 Objektorientierte Architekturen

08 Objektorientiertes Testen und Test-Driven Development
09 Refactoring
10 Buildmanagement
11 Versions- und Fehlermanagement
12 Sotware- und Architekturmetriken
13 Dependency Injection

25 IT-Recht IT Law	
Semester	5
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Karl Wolfhart Nitsch, TH Lübeck
Lerngebiet	Fachübergreifende Grundlagen
Teilnahmevoraussetzungen	keine
Lernergebnisse	Die Studierenden können • die wichtigsten gesetzlichen Regelungen des IT- und Computerrechts nennen und deren Regelungsinhalte erläutern. • rechtliche Probleme des IT- und Computerrechts im Hinblick auf Risiken von Unternehmen und Privatpersonen einordnen. • verschiedene rechtliche Sachverhalte im Bereich des IT-und Computerrechts aufgrund bestimmter rechtlicher Kriterien vergleichen oder bewerten. • die Rechtsvorschriften des IT- und Computerrechts nach methodisch erlernten Regeln auf konkrete Fallgestaltungen anwenden.
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme mindestens 50%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	In der Präsenzveranstaltung werden unter Zugrundelegung der begleitenden Studienmaterialien praktische Übungen im Umgang mit Gesetzen aus dem Bereich des IT- und Computerrechts anhand anwendungsbezogener Fallbeispiele aus dem Lehrgebiet des Studienmoduls durchgeführt.
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform

Literatur	Köhler, Helmut, BGB, Gesetzestext, 85. Auflage, Beck-Texte im dtv, 2020 Marly, Jochen: Praxishandbuch Softwarerecht, 7. Auflage, C.H.Beck, 2018 Nitsch, Karl Wolfhart: Informatikrecht, 5. Auflage, Springer, 2017 Weitnauer, Wolfgang/Mueller-Stöfen, Tilman (Herausgeber): Beck'sches Formularbuch IT-Recht, 5. Auflage, C.H.Beck, 2020 Redeker, Helmut: IT-Recht, 7. Auflage, C.H.Beck, 2020 Schneider, Jochen, IT- und Computerrecht - CompR, Gesetzestexte, 14. Auflage, Beck-Texte im dtv, 2020
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten Es ist erforderlich, studienbegleitend stets die anzuwendenden Gesetze sorgfältig durchzuarbeiten. Als Gesetzessammlung wird zur Anschaffung empfohlen: Textausgabe IT- und Computerrecht, Verlag C. H. Beck

Studieninhalte
1. Verfassungsrechtliche Grundlagen 2. Recht der Telemedien 3. Recht des elektronischen Geschäftsverkehrs 4. IT-Vertragsrecht 5. Schutz des geistigen Eigentums (Urheberrecht/Urheberrechtsschutz von Computerprogrammen, Patentrecht, Designrecht, Markenrecht) 6. Wettbewerbs- und Werberecht im Internet 7. Datenschutzrecht 8. Computerstrafrecht 9. Domainrecht

26 Praxisprojekt Practice-based Project	
Semester	5
Dauer (Semester)	einsemestrig
Credit Points	15
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Jeweils betreuender Professor/ betreuende Professorin
Lerngebiet	Fachspezifische Vertiefung (Berufspraktische Tätigkeit)
Teilnahmevoraussetzungen	Zuvor sollen die Module des 1. bis 4. Fachsemesters absolviert worden sein.
Lernergebnisse	Nach dem erfolgreichen Abschluss des Studienmoduls, sind die Studierenden in der Lage, • die im Studium vermittelten Kenntnisse und Fertigkeiten in einem berufsbezogenen Umfeld einzusetzen, • ein umfangreiches, komplexes, praxisorientiertes Projekt mit den im Studium erlernten Methoden eigenständig zu bearbeiten, • sich ihre Arbeitsaufgaben und ihre Arbeitszeiten auch über einen längeren Zeitraum hinweg selbständig zu organisieren, • den Projektablauf fortlaufend anhand eines Berichtshefts zu dokumentieren und dem lokalen Projektbetreuer zu präsentieren, • das Projektergebnis abschließend in angemessenem Umfang und angemessener wissenschaftlicher Tiefe in einem Projektbericht zu dokumentieren, • das Projektergebnis in einem mediengestützten Vortrag abschließend zu präsentieren.
Prüfungsvorleistung	keine
Medien-/ Lernform	Individuelle Betreuung der Studierenden je nach Aufgabenstellung in der Praxisphase mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chat, Webkonferenzen, Einsendeaufgaben u. a.).
Arbeitsaufwand	Projektbearbeitung inkl. Berichterstellung: ca. 438 h Webkonferenzteilnahme: ca. 12 h
Präsenzart	In Online-Konferenz möglich
Präsenzinhalte	Individuelle Betreuung der Studierenden je nach Aufgabenstellung im Praxisprojekt
Prüfungsform	Schriftlicher Projektbericht

Literatur	Wird je nach Aufgabenstellung der Praxisaufgabe gegeben
weitere Hinweise	Der Bericht wird i. d. R. auf Deutsch verfasst.

Studieninhalte
Das Praxisprojekt ist ein in das Studium integrierter, von der Hochschule geregelter, inhaltlich bestimmter, betreuter Ausbildungsabschnitt, in dem die Studierenden ein komplexes, praxisorientiertes Projekt mit den im Studium erlernten Methoden im Zusammenhang bearbeiten. Das Praxisprojekt findet in einem Betrieb, einer anderen Einrichtung der Berufspraxis oder an einer Fachhochschule des Verbundes "Virtuelle Fachhochschule" statt.

27 Betriebswirtschaftslehre Business Administration	
Semester	6
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Tim Voigt, Technische Hochschule Lübeck
Lerngebiet	Allgemeinwissenschaftliche Ergänzungen (Wirtschaftswissenschaften)
Teilnahmevoraussetzungen	keine
Lernergebnisse	Die Studierenden können • grundlegende Methoden und Modelle zur Entscheidungsfindung erklären und anwenden (Entscheidungstheorie, Spieltheorie). • typische Entscheidungen zur betrieblichen Konstitution (konstitutive Entscheidungen) systematisieren, darstellen und in Bezug auf ihre ökonomische Wirkung bewerten (Standort, Rechtsform und Unternehmensverbindungen). • mit Hilfe der gängigen Methoden der Organisationsgestaltung sowie des Personalmanagements betriebliche Organisationsstrukturen darstellen und Stellenbesetzungs- bzw. Personalbeschaffungsentscheidungen vorbereiten. • die gängigen Optimierungsverfahren (ABC-Analyse, Portfolioanalyse, Produktionsfunktionen) in den Phasen des Prozesses der betrieblichen Leistungserstellung (Entwicklung-Beschaffung-Produktion-Absatz) anwenden. • grundsätzliche Aussagen des Jahresabschlusses interpretieren, grundlegende betriebliche Sachverhalte kostenrechnerisch darstellen und Investitions- bzw. Finanzierungsentscheidungen methodisch vorbereiten. • die formalen Entscheidungsstrukturen der Führungsorganisation (Corporate Governance) darstellen sowie deren Einflussmöglichkeiten durch Stakeholder bewerten und die grundlegenden Methoden der strategischen Planung anwenden.
Prüfungsvorleistung	Einsendeaufgabe
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen

Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Prüfung: 120 Minuten
Präsenzart	In Online-Konferenz möglich
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Wöhe, Günter; Döring, Ulrich; Brösel, Gerrit (2016): Einführung in die allgemeine Betriebswirtschaftslehre. 26., überarbeitete und aktualisierte Auflage. München: Verlag Franz Vahlen Thommen, Jean-Paul; Achleitner, Ann-Kristin (2013): Allgemeine Betriebswirtschaftslehre. 7., aktualisierte Auflage. Wiesbaden: Springer Gabler. Vahs, Dietmar; Schäfer-Kunz, Jan (2015): Einführung in die Betriebswirtschaftslehre. 7. überarbeitete Auflage. Stuttgart: Schäffer Poeschel. Jung, Hans (2016): Allgemeine Betriebswirtschaftslehre. 13., aktualisierte Auflage. Berlin, Boston: De Gruyter Oldenbourg. Straub, Thomas (2015): Einführung in die allgemeine Betriebswirtschaftslehre. 2., aktualisierte und erweiterte Auflage. Hallbergmoos: Pearson Oehlrich, Marcus (2013): Betriebswirtschaftslehre – Eine Einführung am Businessplan-Prozess, 3. überarbeitete und aktualisierte Auflage, München: Vahlen. Paul, Joachim (2015): Praxisorientierte Einführung in die Allgemeine Betriebswirtschaftslehre. Mit Beispielen und Fallstudien. 3., aktualisierte Auflage. Wiesbaden: Springer Gabler. Schweitzer, Marcell; Baumeister, Alexander (2015): Allgemeine Betriebswirtschaftslehre. Theorie und Politik des Wirtschaftens in Unternehmen. 11., völlig neu bearbeitete Auflage. Berlin: Erich Schmidt Verlag
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
Einordnung und Entwicklung der BWL • BWL als Wissenschaft • Entwicklung des Faches • Die Teilgebiete der BWL **Ziele, Kennzahlen und Betriebstypen** • Der Zielbildungsprozess • Betriebliche Ziele • Das ökonomische Prinzip

- Betriebstypologie

Betriebliche Entscheidungen
- Betrieblicher Entscheidungsprozess
- Grundelemente einer Entscheidungssituation
- Entscheidungsmodelle
- Entscheidungsbaum und mehrstufige Entscheidungsmodelle
- Entscheidungen bei Spielsituationen

Konstitutive Entscheidungen
- Begriffsbestimmung
- Standortentscheidungen
- Rechtsformentscheidungen
- Entscheidungen zu Unternehmensverbindungen

Personal und Organisation
- Grundlegende Ziele und Aufgaben
- Stellenbildung und Personalplanung
- Führungsorganisation und Personaleinsatz
- Klassische Organisationsformen

Finanz- und Rechnungswesen
- Überblick
- Externes Rechnungswesen: Der Jahresabschluss
- Internes Rechnungswesen: Die Kostenrechnung
- Finanzwesen

Betrieblicher Leistungsprozess
- Der betriebliche Leistungsprozess im Überblick
- Beschaffung und Materialwirtschaft
- Produktionswirtschaft und Fertigung
- Absatzwirtschaft und Marketing

28 Abschlussprüfung

Final Examination Module

Semester	6
Credit Points	12 + 3 (Bachelorarbeit + mündliche Abschlussprüfung)
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester
Modulverantwortliche(r)	Jeweils betreuender Professor/ betreuende Professorin
Teilnahmevoraussetzungen	Die Bachelorarbeit kann nur bearbeiten, wer alle Studienmodule bis auf Studienmodule im Umfang von höchstens 20 Leistungspunkten bestanden hat. Die noch nicht abgeschlossenen Studienmodule müssen bei Bearbeitungsbeginn der Bachelorarbeit belegt sein. Die mündliche Abschlussprüfung darf erst durchgeführt werden, wenn a) die Bachelorarbeit und b) alle Pflichtmodule und im erforderlichen Umfang Wahlpflichtmodule des Studiengangs bestanden wurden.
Lernergebnisse	Durch die Bachelorarbeit soll der/die Studierende zeigen, dass er/sie in der Lage ist, innerhalb einer vorgegebenen Frist ein anwendungsorientiertes Problem aus seinem/ihrem Fach selbständig mit wissenschaftlichen Methoden und praxisgerecht zu bearbeiten. Iin der mündlichen Abschlussprüfung sollen Inhalte und Ergebnis der Bachelorarbeit durch den Studierenden bzw. die Studierende mündlich vertreten werden.
Medien-/ Lernform	Prüfungsarbeit mit individueller Betreuung
Arbeitsaufwand	Anfertigen der schriftlichen Bachelorarbeit: 360 Stunden, mündliche Abschlussprüfung: 30-45 Minuten
Literatur	Wird je nach Aufgabenstellung der Bachelorarbeit gegeben
weitere Hinweise	Die Bachelorarbeit ist auf Deutsch anzufertigen, kann aber nach Vereinbarung zwischen Prüfling und Prüfer/in auch in englischer Sprache erfolgen.

Studieninhalte
Der Inhalt der Bachelorarbeit ist abhängig vom ausgegeben Thema. Die mündliche Abschlussprüfung orientiert sich schwerpunktmäßig an den Fachgebieten der Bachelorarbeit. Es soll hierdurch festgestellt werden, ob der/die Studierende gesichertes Wissen in den Fachgebieten, denen die Bachelorarbeit thematisch zugeordnet ist, besitzt und ob er/sie fähig ist, die Ergebnisse der Bachelorarbeit zu verteidigen.

29 Anforderungsanalyse und Modellierung

Requirements Analysis and Modeling

Semester	Wahlpflichtbereich
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Wahlpflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	
Lerngebiet	Fachübergreifende Vertiefung (Informatik)
Teilnahmevoraussetzungen	keine
Lernergebnisse	Nach Abschluss der Lehrveranstaltung sind die Studierenden in der Lage, für neu zu entwickelnde Softwareprodukte oder -services den Problemraum abzugrenzen und eine Lösung zu konzipieren. Weiter sind die Studenten in der Lage die Techniken des Anforderungsmanagements sowie der Modellierung mit UML anzuwenden und die notwendigen Tätigkeiten für spezifische Projekte und Anwendungsdomänen zu planen.
Prüfungsvorleistung	Präsenzteilnahme mindestens 50%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium inkl. Anfertigung der Hausarbeit: ca. 131,5 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Kolloquium: 30 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Lehrstoffübersicht sowie Projekteinführung
Prüfungsform	Hausarbeit mit Kolloquium (30 min)
Literatur	Pohl, Rupp, Basiswissen Requirements Engineering: Aus- und Weiterbildung nach IREB-Standard zum Certified Professional for Requirements Engineering -- Foundation Level, Dpunkt Verlag, 2010 Weikiens, T. Systems Engineering mit SysML/UML: Modellierung, Analyse, Design. Rupp, C.; Queins, S.; Zengler, B. UML 2 glasklar, Praxiswissen für die UML- Modellierung.

weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
Anforderungen und Modellierung Motivation der Anforderungsanalyse Anforderungsanalyse (Grundbegriffe, Aufgaben, Anforderungsanalyse und Anforderungsvalidierung Beschreibung von Anforderungen Anwendungsfälle Lastenheft Modellierung mit UML UML und Objektorientierung Ereignisdikrete Systeme Vorgehensmodelle (MDA, MDD,…) Erweiterungen

30 Automotive Security

Automotive Security

Semester	Wahlpflichtbereich
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Wahlpflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes
Modulverantwortliche(r)	Prof. Dr. Claus Vielhauer, Technische Hochschule Brandenburg
Lerngebiet	Fachspezifische Vertiefung
Teilnahmevoraussetzungen	Empfehlung: Grundlagen IT-Sicherheit
Lernergebnisse	Nach dem erfolgreichen Abschluss des Studienmoduls, erreichen die Studierenden folgende Lernergebnisse. Die Studierenden…. • können Security-by-Design (Sicherheitsaspekte, Bedrohungen und Maßnahmen) im Kontext im und um das Automobil anwenden. • besitzen die Fähigkeit IT-Sicherheitsziele und den Schutzbedarf unter Einbezug von Forensik zu evaluieren. • erwerben das Grundverständnis über Sicherheitsaspekte, Schutzziele und Sicherheitsmaßnahmen in und für Automotive-Systemen, sowie die Fähigkeit diese einzuschätzen. • haben die Befähigung, IT-Sicherheits-Ansätze mit technischen Paradigmen aus anderen Gebieten des Automobilbaus, wie beispielsweise der Safety-Anforderungen, für das Automobil zu kombinieren. • erlangen das technisch/mathematische Wissen zum grundsätzlichen Verständnis von Security-by-Design und der Funktionsweise kritischer Systeme im Automobil und können dieses vermitteln. • verstehen Ausgewählte, exemplarische Verfahren für spezifische Risiken im Detail und können dieses auch an Dritten vermitteln. • besitzen die Fähigkeiten zur Konzeption und Implementierung einfacher Maßnahmen für das Security-By-Design. • haben die Fähigkeiten zur Konzeption der Erfassung und Analyse von Kommunikationsdaten des Fahrzeugs zur Aufklärung von Sicherheitsvorfällen. Fähigkeiten zur Konzeption von Security-Testing zur Evaluation der Wirksamkeit der Security-By-Design-Maßnahmen. • verstehen die Grenzen des Security-by-Design, zum Beispiel aufgrund von Safety Anforderungen und Fehlentscheidungen, datenschutzrechtlichen / ethischen Erwägungen.

	• kennen Methodik und Metrik zur Evaluierung von Angriffsszenarien und Forensik für ausgewählte Komponenten des Automobils. • erwerben die Fähigkeit zur Erstellung von einfachen Security-by-Design Konzepten und Sicherheitsanalysen. • werden im Rahmen von Aufgaben schrittweise (ggf. im Team) exemplarisch automotive Systeme analysieren und Security-by-Design Aspekte kennenlernen.
Prüfungsvorleistung	Gruppenarbeit via Internet, Präsenzteilnahme mindestens 50%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium inkl. Anfertigung der Hausarbeit: ca. 131,5 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Kolloquium: 30 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Inhaltliche Klärung, Besprechung von erweiterten Übungsaufgaben
Prüfungsform	Hausarbeit mit Kolloquium (30 min)
Literatur	Craig Smith, „The Car Hacker's Handbook - A Guide for the Penetration Tester“, No Starch Press, Inc., San Francisco, 2016, ISBN 978-1-59327-703-1 Bundesanstalt für Straßenwesen, Rechtsfolgen zunehmender Fahrzeugautomatisierung, Berichte der Bundesanstalt für Straßenwesen - Fahrzeugtechnik Heft F83, 2012 K. Borgeest, Elektronik in der Fahrzeugtechnik - Hardware, Software, Systeme und Projektmanagement, 2010 978-3-8348-0548-5 Jana Dittmann, Tobias Hoppe, Stefan Kiltz, Sven Tuchscheerer, Elektronische Manipulation von Fahrzeug- und Infrastruktursystemen: Gefährdungspotentiale für die Straßenverkehrssicherheit, Berichte der Bundesanstalt für Straßenwesen Fahrzeugtechnik Heft F78, 2011 European Union Agency For Network And Information Security, Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations , 2016, [Online] https://www.enisa.europa.eu/publications/good-practices-recommendations European Union Agency For Network And Information Security, Cyber Security and Resilience of smart cars, 2017, [Online] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars T. Gasser, C. Arzt, M. Ayoubi, A. Bartels, L. Bürkle, J. Eier, F. Flemisch, D. Häcker, T. Hesse, W. Huber, C. Lotz, M. Maurer, S. Ruth-Schuhmacher, J. Schwarz, W. Vogt, Rechtsfolgen zunehmender

	Fahrzeugautomatisierung, Berichte der Bundesanstalt für Straßenwesen - Fahrzeugtechnik Heft F83 , 2012 Marko Wolf, Security Engineering for Vehicular IT Systems, 2009 978-3-8348-0795-3 Hendrik Schweppe, Security and Privacy in Automotive On-Board Networks, Doktorarbeit, 2012, [Online] www.eurecom.fr/en/publication/3852/download/rs-publi-3852.pdf M. Maurer, J. Gerdes, B. Lenz, H. Winner, Autonomes Fahren -Technische, rechtliche und gesellschaftliche Aspekte, 2015 978-3-662-45853-2 H. Wallentowitz, K. Reif, Handbuch Kraftfahrzeug - Grundlagen, Komponenten, Systeme, Anwendungen, 2006 978-3-528-03971-4, 2011 W. Zimmermann, R. Schmidgall, Bussysteme in der Fahrzeugtechnik - Protokolle, Standards und Softwarearchitektur, 2014 978-3-658-02418-5, 2014 S. Pischinger, U. Seiffert, Vieweg Handbuch Kraftfahrzeugtechnik - 8. aktualisierte und erweiterte Auflage, 2016 978-3-658-09527-7, 2016 Zusätzliche Referenzen innerhalb der Lerneinheiten
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
Automtotive Security ist ein wichtiges Thema bei der immer weiter fortschreitenden Digitalisierung von Fahrzeugen und Anzahl von Schnittstellen in das Fahrzeug als auch vom Fahrzeug nach außen. Neben den Vorteilen zum Beispiel an funktionaler Sicherheit und Komfort sind auch Nachteile, insbesondere durch eine Bedrohung der eingesetzten IT-Systeme bezüglich der IT-Sicherheit, zu verzeichnen. In der Literatur finden sich dazu bereits eine Vielzahl an bekannt geworden Schwachstellen und Bedrohungen. Um die Besonderheiten zu verstehen, wird eine Pauschalisierung des automotiven IT-Systems vorgenommen. Ausgangspunkte für die Pauschalisierung sind mechatronischen Betrachtungsweisen, wonach IT-Systeme Mess-, Steuer- und Regelkreise unter Nutzung von Sensoren umsetzen. Elektronischen Steuergerät (Electronic Control Unit, ECU) nehmen Berechnungen, Aktoren mit elektrischen Signalen zum Zweck der Beeinflussung der physischen Umwelt ansteuern. Die Mess-, Steuer- und Regelkreise und die von ihnen realisierten Funktionalitäten werden in Komponenten zusammengefasst und die Aspekte von Security an verschiedenen Beispielen erläutert.. Dieses Lernmodul führt dazu in dieses Gebiet ein, in dem es Automotive Security vor dem Hintergrund von Safety motiviert und Fahrzeugkomponenten in ihrer Funktion erläutert. Potentielle Sicherheitsaspekte, Bedrohungen, Risiken und den resultierenden Schutzbedarf werden vermittelt, sowie exemplarisch Verfahren für ausgewählte Komponenten und ausgewählte Sicherheitsmaßnahmen im Detail beleuchtet. Am Beispiel des automatisiertes und vernetzten Fahrens wird das Zusammenspiel von Safety und Security betrachtet. Die behandelten Themen werden zusammengefasst und Grenzen aufgezeigt. **Lerneinheiten** • Motivation und Einführung zu Automotive Security und das Zusammenspiel mit Safety

- Überblick IT-System Automobil: pauschalisierte Komponentenklassen und Komponenten
- Überblick Security: Sicherheitsaspekte, Schutzziel und Schutzobjekte im Automobile
- Exemplarische Bedrohungen, Schwachstellen, Risiken und deren Bewertung, ausgewählte Maßnahmen an exemplarisch ausgewählten Komponentenklassen und Beispiele zu automatisierten und vernetztem Fahren
- Zusammenfassung
- Präsentation und Vergabe von ausgewählten Themen für die studentischen Hausarbeiten

31 Biometrie Biometrics	
Semester	Wahlpflichtbereich
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Wahlpflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Claus Vielhauer, Technische Hochschule Brandenburg
Lerngebiet	IT-Sicherheit
Teilnahmevoraussetzungen	empfohlen: Grundlagen IT-Sicherheit, Algorithmen und Datenstrukturen
Lernergebnisse	Nach dem erfolgreichen Abschluss des Studienmoduls, erreichen die Studierenden folgende Lernergebnisse. Die Studierenden…. • können Mustererkennungsverfahren im Kontext der Biometrie anwenden. • können experimentelle Evaluationen unter Einbezug von statistischen Grundprinzipien durchführen. • bilden ein Grundverständnis über Sicherheitsaspekte in und für Biometrie-Systeme ausbilden. Sie besitzen außerdem die Fähigkeit diese einzuschätzen. • können biometrische Ansätze mit technischen Paradigmen aus anderen Gebieten der IT Sicherheit, wie beispielsweise der Kryptographie, für ein spezifisches Systemziel kombinieren. • haben das technisch/mathematische Wissen zum grundsätzlichen Verständnis von Funktionsweise der Biometrie ist und können dieses vermitteln. • verstehen im Detail ausgewählte, exemplarisch Verfahren für spezifische biometrische Modalitäten können dieses auch Dritten vermitteln. • haben die Fähigkeiten zur Konzeption und Implementierung einfacher Mustererkennungsverfahren für die Biometrie, einschließlich Merkmalsextraktion und -verifikation anhand von Ähnlichkeitsberechnungen. • verstehen die Grenzen der Biometrie, zum Beispiel aufgrund von inhärenten Fehlentscheidungstendenzen und datenschutzrechtlichen / ethischen Erwägungen.

	• können für generelle Evaluierungsaufgaben Methodik und Metrik zur experimentellen Evaluierung (einschließlich Angriffsszenarien) solcher Systeme für generelle Evaluierungsaufgaben einsetzen. • erwerben die Fähigkeit zur Erstellung von Konzepten des Aufbaus, Evaluierung und Anwendung von biometrischen Systemen zur Benutzerauthentifizierung. • werden im Rahmen der praktischen Übungen schrittweise im Team exemplarisch biometrische Systeme entwerfen, implementieren ...
Prüfungsvorleistung	Einsendeaufgabe, mind. 50% Päsenzteilnahme
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chat, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen.
Arbeitsaufwand	Selbststudium: ca. 130 h Präsenzteilnahme: ca. 6 h Webkonferenzteilnahme ca. 12 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Claus Vielhauer: Biometric User Authentication for IT Security: From Fundamentals to Handwriting, ISBN 0-387-26194-X, 2006 (in Englisch) David D. Zhang: Automated Biometrics, ISBN 0-7923-7856-3, 2000 (in Englisch) Behrens Michael, Richard Roth: Biometrische Identifikation, Vieweg+Teubner Verlag, 978-3-322-90844-5, 2001 Anil K. Jain, Patrick Flynn , Arun A. Ross: Handbook of Biometrics, Springer, ISBN-13: 978-0387710402, 2007 (in English) Zusätzliche Referenzen innerhalb der Lerneinheiten
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
In der jüngsten Vergangenheit haben biometrische Benutzerauthentifikationsverfahren ein enormes Interesse seitens Forschung, Industrie und Gesellschaft gefunden und bilden heute eine eigene technische Domäne innerhalb der IT Sicherheit. Die Methoden zur automatischen Bestimmung oder Bestätigung von menschlichen Identitäten basierend auf deren physiologischen oder verhaltensbasierten Eigenschaften sollen zur Lösungen von Problemstellungen der heutigen Informationstechnologie dienen, insbesondere der Bindung von realen Identitäten an virtuelle. Diese Lernmodul führt in dieses Gebiet ein, indem die technisch/mathematischen Konzepte vermittelt werden, sowie exemplarisch Verfahren für spezifische biometrische Modalitäten im Detail beleuchtet. Darüber hinaus befasst sich der Kurs mit den Grenzen der Biometrie, zum Beispiel aufgrund von inhärenten Fehlertendendenzen und datenschutzrechlichen / ethischen Erwägungen. Ferner werden in

die Methodik und Metrik zur experimentellen Evaluierung (einschließlich Angriffsszenarien) solcher Systeme eingeführt und Einblicke in die Kombination mit Paradigmen aus anderen Gebieten der IT Sicherheit, wie beispielsweise der Kryptographie, gegeben

Lehreinheiten

1. Motivation und Einführung
2. Sicherheitsaspekte zur Systemsicherheit
3. Technische und mathematische Grundlagen biometrischer Systeme
4. Fehlerraten, Erkennungsgenauigkeit und Fälschungssicherheit
5. Multimodal Biometrics and Multifactor Authentication: Fusionstrategien zur Erhöhung der Sicherheit
6. Datenschutzaspekte biometrischer Systeme
7. Biometrie & Kryptographie
8. Evaluierung von und Angriffe auf biometrische Systeme
9. Praktische Beispiele zu Biometrie und Sicherheit in der Praxis

32 Cloud Computing

Cloud Computing

Semester	Wahlpflichtbereich
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Wahlpflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Dr.-Ing. Thomas Preuss, Technische Hochschule Brandenburg
Lerngebiet	Fachübergreifende Grundlagen
Teilnahmevoraussetzungen	Empfehlung: Grundlagen der Programmierung 1 + 2, Computerarchitektur und Betriebssysteme, Rechnernetze Grundlagen, Datenbanken
Lernergebnisse	Die Studierenden kennen und verstehen die Spezifika und Grundkonzepte von Cloud-Systemen. Sie sind in der Lage, die Notwendigkeit, die Vorteile aber auch die Probleme beim Einsatz dieser Systeme abzuschätzen und zu bewerten. Die Studierenden können die grundlegenden Technologien zur Entwicklung von verteilten Anwendungen in der Cloud anwenden. Im Rahmen der praktischen Übungen werden die Studenten schrittweise eine verteilte Anwendung in der AWS-Cloud unter Verwendung ausgewählter Technologien entwerfen und implementieren und somit Problemlösungs- und Methodenkompetenz in beiden Bereichen erwerben.
Prüfungsvorleistung	keine
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium inkl. Anfertigung der Hausarbeit: ca. 137,5 h Webkonferenzteilnahme: ca. 12 h Kolloquium: 30 Minuten
Prüfungsform	Hausarbeit mit Kolloquium (30 min)
Literatur	T. Erl; Z. Mahmood; R. Puttini: Cloud Computing: Concepts, Technology & Architecture, Pearson 2013. M. J. Kavis: Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, & IaaS), Wiley, 2014.

	N. Kumar, P. C. P. Bhatt: Cloud Computing: Concepts and Practices, Springer, 2018. A. Homer et. al.:Cloud Design Patterns, Microsoft patterns & practices, 2014.
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
• Virtualisierung • Motivation und Probleme beim Einsatz verteilter und Cloud-basierter Systeme Cloud Service Models (IaaS, PaaS, SaaS) • Cloud Delivery Models (Public, private, community, hybrid) • Abrechnungsmodelle in der Cloud • Skalierung & Replikation • AWS • Compute Services (ec2, Lambda, ecs) • Storage Services (S3 / Cloud Front, EFS, EBS, Storage Gateways) • Identity and Access Management (IAM) and Cloud Security • Load Balancing & Autoscaling • Monitoring (Cloud Watch) • Network Virtualization (VPC) • Open Stack • Abrechnungsmodelle und SLAs • Webservices (REST & SOAP) • Container-Technologien, z. B. Docker, Kubernetes • Aktuelle Trends Für das Modul wird ein AWS-Account, z. B. im Rahmen von AWS Educate (https://awseducate.com) benötigt.

33 Ethical Hacking

Ethical Hacking

Semester	Wahlpflichtbereich
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Wahlpflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. rer. nat. Reiner Creutzburg, Technische Hochschule Brandenburg
Lerngebiet	Fachspezifische Grundlagen (Informatik)
Teilnahmevoraussetzungen	Empfehlung: Computerarchitektur und Betriebssysteme, Internettechnologie, Rechnernetze, Netzwerksicherheit, Grundlagen der IT-Sicherheit
Lernergebnisse	Nach dem erfolgreichen Abschluss des Studienmoduls, sind die Studierenden in der Lage, • sich in die Denk- und Arbeitsweise potenzieller Angreifer von IT-Systemen hineinzuversetzen und Angriffsmuster zu erkennen, zu analysieren und Gegenmaßnahmen einzuleiten, • sich auf der Plattform Hacking-Lab.com mit realen Angriffsszenarien und dem Ausnutzen von Schwachstellen auseinanderzusetzen und dabei selbst die Rolle des Angreifers in einer geschützten Umgebung zu übernehmen, • die wachsende Bedeutung von Cyber-Sicherheit zu erkennen und ihr Verhalten dementsprechend zu überdenken und ggf. anzupassen.
Prüfungsvorleistung	keine
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium inkl. Erbringung der Prüfungsleistungen: ca. 138 h Webkonferenzteilnahme: ca. 12 h
Präsenzinhalte	Inhaltliche Klärung; Vorstellung Lösungskonzept des Projekts
Prüfungsform	Portfolioprüfung
Literatur	Oriyano: CEH v9: Certified Ethical Hacker Version 9 Study Guide, Sybex; 3rd edition, 2016 M. Walker: CEH Certified Ethical Hacker Bundle, Third Edition (All-

	In-One), McGraw-Hill Education; 3rd edition, 2017 P. Engebretson: The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy, Syngress; 2nd edition, 2013 M. Messner: Hacking mit Metasploit: Das umfassende Handbuch zu Penetration Testing und Metasploit, dpunkt.verlag 2015 P. Kraft; A. Weyert: Network Hacking - Professionelle Angriffs - und Verteidigungstechniken gegen Hacker und Datendiebe, Francis 2015 Vorlesungsskript Creutzburg
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
Die Studierenden können einen Überblick zur Bedeutung und zu Methoden und Tools des Ethical Hacking geben und erste Erfahrungen anwenden. Sie sind in der Lage Risiken einzuschätzen, Bedrohungen abzuwägen und Maßnahmen zur Sicherung von Rechnernetzen und –anwendungen zu ergreifen. Die Studenten erwerben praktische Fähigkeiten beim Ethical Hacking durch das Lösen von Aufgaben im Hacking-Lab (www.hacking-lab.com). Sie haben Verständnis für die Rolle und den Einsatz eines „Ethical Hacker“ im Unternehmen. **Lehreinheiten** 1. Ethical Hacking 2. Footprinting and Reconnaissance 3. Scanning Networks 4. Enumeration 5. System Hacking 6. Malware Threats 7. Sniffing 8. Social Engineering. 9. Denial-of-Service 10. Session Hijacking 11. Hacking Webservers 12. Hacking Web Applications 13. SQL Injection 14. Hacking Wireless Networks

34 Informationsmanagement

Information Management

Semester	Wahlpflichtbereich
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Wahlpflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Dipl.-Wirt.-Inform. Jan Hannemann, Technische Hochschule Brandenburg; Dipl.-Wirt.-Inf. Kai Skrabe, Technische Hochschule Brandenburg
Lerngebiet	Fachübergreifende Grundlagen (Informatik , Grundlagen des Informationsmanagements)
Teilnahmevoraussetzungen	keine
Lernergebnisse	Die Studierenden können (allg.)… • Kenntnisse zum Aufbau des Sachgebiets und seinen wesentlichen Elementen erwerben • Kenntnisse methodische Grundlagen im Sachgebiet erwerben • Fähigkeiten zur Anwendung von Methoden und Elementen des Sachgebiets erwerben • Fähigkeiten zur Lösung komplexer Aufgabenstellungen in Betrieben oder Organisationen erwerben • Fähigkeiten zu empirischer Datenerhebung im Betrieb erwerben • Fähigkeiten zur Arbeit in Kleingruppen erwerben und vertiefen … sind in der Lage… • ein Problembewusstsein für die Folgen der Entwicklung der Informationsgesellschaft herauszubilden • betriebliche Informationssysteme als komplexe Anwendungen zu erläutern • Informationsmanagement als Führungsaufgabe in Unternehmen zu verstehen • die Ziele/Funktionen/Aufgaben des Informationsmanagements und des Informationsmanagers strukturiert darzustellen • den Zusammenhang zwischen IuK-Systemen und ausgewählten Informationsmanagementkonzepten im Unternehmen herzustellen • unternehmensbezogene Methoden und Techniken für ein erfolgreiches Informationsmanagement zu entwickeln und einzusetzen

	• aktuelle Tendenzen der Entwicklung des Informationsmanagements in Unternehmen vorzustellen
Prüfungsvorleistung	Gruppenarbeit via Internet, Präsenzteilnahme mindestens 50%
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium inkl. Anfertigung der Hausarbeit: ca. 131,5 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Prüfung: 30 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Gruppenbildung und -rollen, Fallstudienaufbau Aufgabenerläuterung Fallstudienmethodik
Prüfungsform	Hausarbeit mit Kolloquium (30 min)
Literatur	Krcmar, H.; Informationsmanagement; 5. vollst. überarb. u. erw. Aufl. 2010; Berlin Laudon, K.; Laudon, J.P.; Schoder, D; Wirtschaftsinformatik - Eine Einführung; 2. aktualisierte Auflage 2010; Pearson Education Deutschland GmbH; München, Boston u. a. Heinrich, L.J.; Stelzer, D.; Informationsmanagement - Grundlagen, Aufgaben, Methoden; 10. Auflage 2011; Oldenbourg-Verlag; München, Wiesbaden …weitere: siehe Modul Literaturquellen
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
1 Exkurs - Grundlagen Fallstudienarbeit 2 Einführende Fallstudie: Gebäudemanagement - Intelligente, IT-gestützte Heizungssysteme 3 Grundlagen der Informationswissenschaft und Informationswirtschaft 4 Theoretische Grundlagen des Informationsmanagements 5 Informationsmanagement in Organisationen 6 Aufgabenebenen des Informationsmanagements 7 Aufgaben und Funktion des Informationsmanagers (CIO) 8 Methodiken und Techniken des Informationsmanagements 9 Daten- und Informationsqualität - Definitionen, Dimensionen und Begriffe 10 IT-Controlling 11 Informationsmanagement - Trends und Entwicklungen, Chancen und Risiken 12 Nachhaltigkeit und Informationsmanagement

35 Multimediatechnik Multimedia Technology	
Semester	Wahlpflichtbereich
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Wahlpflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Thomas Lemke, Hochschule Emden/Leer
Lerngebiet	Fachübergreifende Vertiefung
Teilnahmevoraussetzungen	Empfehlung: Grundlagen der Mathematik, Grundlagen der Programmierung 1 + 2
Lernergebnisse	Die Studierenden kennen die grundlegenden algorithmischen Parameter der Medien, wie z.B. Abtastrate, Zeilenzahl. Sie verstehen die mathematischen Beschreibungen nachrichtentechnischer Systeme durch Größen wie Dezibel, Aussteuerung, Abtastraten, Quantisierung usw. Die Studierenden sind in der Lage die mathematischen Größen zu berechnen. Sie verstehen Grundprinzipien analoger und (unkomprimierter) digitaler Medien. Sie können digitale Medien in der Medienproduktion anwenden. Die Studierenden sind in der Lage die Probleme beim Einsatz analoger/ digitaler Medien in der Medienproduktion zu analysieren und zu bewerten. Sie entwickeln ein Verständnis für die Anwendung unterschiedlicher Medien in der Medieninformatik.
Prüfungsvorleistung	keine
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 133 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 3 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit

Präsenzinhalte	Ausgewählte Themenbereiche des Lehrstoffs, Insbesondere: Dezibel, Abtastung, Quantisierung, Videosignal, HDTV; Diskussion über Fragen der Studierenden
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Görne, Thomas 2015: Tontechnik. 4. Aufl., Hanser Verlag, München Dickreiter, Michael at al. 2014: Handbuch der Tonstudiotechnik. 8. Aufl., De Gruyter/Saur, Berlin, Boston Bühler, Peter; Schlaich, Patrik; Sinner Dominik 2018: Digitale Farbe. Springer Verlag, Berlin Bühler, Peter; Schlaich, Patrik; Sinner Dominik 2017: Digitale Bild. Springer Verlag, Berlin Böhringer, Joachim; Bühler, Peter; Schlaich, Patrik 2011: Kompendium der Mediengestaltung – Konzeption und Gestaltung. 5. Aufl., Springer Verlag, Berlin Böhringer, Joachim at al. 2014: Kompendium der Mediengestaltung – II. Medientechnik. 6. Aufl., Springer Verlag, Berlin Schmidt, Ulrich 2013: Professionelle Videotechnik. 6. Aufl. Springer Vieweg, Berlin Heidelberg Poynton, Charles 2012: Digital Video and HD. 2. Aufl., Morgan Kaufmann, Amsterdam Boston usf. Greule, Roland 2015: Licht und Beleuchtung im Medienbereich. Hanser Verlag, München
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
1. Einleitung 2. Audio 2.1 Analoge Audiosignale 2.2 Digitale Audiosignale 2.3 Audio-Gerätetechnik 3. Grafik 3.1 Einführung 3.2 Vektorgrafik 3.3 Rastergrafik 3.4 Bearbeitung im Werbereich 3.5 Bearbeitung im Definitionsbereich 3.6 Bearbeitung im Farbraum 3.7 Grafik-Gerätetechnik 4. Video 4.1 Monochromes Fernsehen 4.2 (Analoges Farbfernsehen) 4.3 Digitales Fernsehen 4.4 HDTV

4.5 Bildseitenverhältnis
4.6 Digital Cinema
4.7 UHDTV
4.8 Video-Gerätetechnik
5. Multimedia-Dateiformate
5.1 WAVE-File
5.2 Tagged Image File Format
6. Grundlagen
6.1 Physikalische und physiologische Grundlagen
6.2 Dezibel
6.3 Digitalisierung
6.4 Farbmischung
6.5 Farbräume

7. Ausblick

36 Objektorientierte Skriptsprachen

Object-oriented Scripting Languages

Semester	Wahlpflichtbereich
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Wahlpflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Dr.-Ing. Thomas Preuss, Technische Hochschule Brandenburg
Lerngebiet	Fachübergreifende Vertiefung
Teilnahmevoraussetzungen	empfohlen: Datenbanken, Webprogrammierung
Lernergebnisse	Die Studierenden kennen die Grundprinzipien von objektorientierten Skriptsprachen. Sie kennen die Konzepte der objektorientierten Programmierung in Python und können diese sicher in Kombination mit anderen Technologien (Webanwendungen, CLI, TK, Spieleprogrammierung) anwenden. Die Studierenden sind in der Lage gängige Bibliotheken, Frameworks und Entwurfsmuster auf ihre Eignung für komplexe Anwendungen zu untersuchen und diese anzuwenden.
Prüfungsvorleistung	keine
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium inkl. Erbringung der Prüfungsleistung: ca. 138 h Webkonferenzteilnahme: ca. 12 h
Prüfungsform	Portfolioprüfung
Literatur	Michael Weigend: Python 3: Lernen und professionell anwenden, mitp Professional, 2016 Johannes Ernesti, Peter Kaiser: Python 3: Das umfassende Handbuch: Sprachgrundlagen, Objektorientierung, Modularisierung, 2015 Al Sweigart: Automate the boring Stuff with Python, No Starch Press, 2017. (https://automatetheboringstuff.com/)
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
• Grundlagen von Skriptsprachen • Einführung Python • Objektorientierte Programmierung in Python • Systemadministration mit Python (CLI) • 2D-Spiele mit PyGame • GUI-Programmierung mit Tkinter • Anwendung des Django-Framework • Skripting, Automatisierung und Erweiterung

37 Programmierung in C++

Programming using C++

Semester	Wahlpflichtbereich
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Wahlpflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Friedhelm Mündemann, Technische Hochschule Brandenburg; Jeweils betreuender Professor/ betreuende Professorin
Lerngebiet	Fachübergreifende Grundlagen (Informatik)
Teilnahmevoraussetzungen	keine
Lernergebnisse	Die Teilnehmerinnen und Teilnehmer werden befähigt, die Grundlagen einer objektorientierten Programmiersprache in Theorie und Praxis zu erlernen und zur Lösung von einfachen Anwendungsproblemen der Wirtschaftsinformatik einsetzen zu können.
Prüfungsvorleistung	Einsendeaufgabe
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.)
Arbeitsaufwand	Selbststudium: ca. 143,5 h Webkonferenzteilnahme: ca. 6 h Prüfung: 90 Minuten
Prüfungsform	Klausur (90 min.)
Literatur	Dirk Louis: C++: Das komplette Starterkit für den einfachen Einstieg in die Programmierung, Hanser, 1. Auflage, 2014 Kirch-Prinz Ulla, Kirch Peter: C++ Lernen und professionell anwenden, mitp, 7.Auflage, 2015 Willemer Arnold: C++. Der Einstieg, Wiley, 1.Auflage, 2013
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
Grundlagen der OO C++-Programmierung C++-Programmierumgebung

Das erste C++-Programm
Basis-Syntax, Teil1
- Ausdruck und Anweisung
- Datentypen und Variablen
- Rechenoperatoren
- Ein- und Ausgabe

Klassenkonzept in C++
- Attribute einer Klasse in C++
- Methoden einer Klasse in C++

Basis-Syntax, Teil2
- Felder
- Kontrollstrukturen

Spezielle Klasseneigenschaften und -methoden
- Konstruktoren/Destruktoren
- Elementinitialisierungsliste
- Überladen von Funktionen
- Klassenvariablen

Vererbung
- Deklaration und Zugriffsrechte
- Initialisierung
- Konstruktoren und Destruktoren bei Vererbung

Fortgeschrittene Programmierkonzepte der Objektorientierung
- Basissyntax C++ (Wiederholung)
- Dynamische Speicherverwaltung
- Dynamische Datenstrukturen
- Polymorphismus
- Operator-Überladung
- Templates

Dateiverarbeitung

38 Projektmanagement

Project Management

Semester	Wahlpflichtbereich
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Wahlpflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr.-Ing. habil. Michael Syrjakow, Technische Hochschule Brandenburg
Lerngebiet	Fachübergreifende Grundlagen
Teilnahmevoraussetzungen	empfohlen: Interesse an Projektarbeit (Planen, Steuern und Kontrollieren von Projekten)
Lernergebnisse	Nach Abschluss des Moduls sind die Studierenden in der Lage, ein Projekt (insbesondere Softwareprojekt) zu planen, zu steuern und zu kontrollieren. Darüber hinaus sind sie für das wichtige Problem der Mitarbeiterführung und -motivation sensibilisiert. Sie kennen den Prozess der Projektabwicklung, können Gefahren für den Projekterfolg identifizieren und sind in der Lage, die im Projektteam ablaufende sozialpsychologischen Prozesse zu reflektieren. Sie können grundlegende Methoden und Techniken des Projektmanagements erklären und darauf basierende Werkzeuge sicher bedienen.
Prüfungsvorleistung	Einsendeaufgabe
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium inkl. Anfertigung der Hausarbeit: ca. 134,5 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 3 h Prüfung: 30 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Diskussionen, Präsentationen, Besprechung der Übungsaufgaben und gemeinsame Bearbeitung weiterer Aufgaben, Klärung inhaltlicher Fragen, Prüfungsvorbereitung
Prüfungsform	Hausarbeit mit Kolloquium (30 min)

Literatur	Andler, N.: Tools für Projektmanagement, Workshops und Consulting: Kompendium der wichtigsten Techniken und Methoden, Publicis Publishing, 2015, 6. Auflage. Buhl, A.: Grundkurs Software-Projektmanagement: Einführung in das Management objektori¬entierter Projekte, Carl Hanser Verlag, 2004. Patzak, u.a.: Projektmanagement: Leitfaden zum Management von Projekten, Projektportfo¬lios und projektorientierten Unternehmen, Linde Verlag, 2014, 6. Auflage. Peipe, S.: Crashkurs Projektmanagement - inkl. Arbeitshilfen online: Grundlagen für alle Projektphasen, Haufe Lexware, 2018. Rosenstock, J.: Microsoft Project 2016 - Das umfassende Handbuch, Rheinwerk Computing, 2016. Tiemeyer, E.: Handbuch IT-Projektmanagement: Vorgehensmodelle, Managementinstru¬mente, Good Practices, Carl Hanser Verlag, 2018. Timinger H.: Modernes Projektmanagement: Mit traditionellem, agilem und hybridem Vorgehen zum Erfolg, Wiley-VCH, 2017, 1. Auflage. Vigenshow, u.a.: Soft Skills für IT-Führungskräfte und Projektleiter: Softwareentwickler führen und coachen, Hochleistungsteams aufbauen, dpunkt.verlag, 2016, 3. aktualisierte und ergänzte Auflage.
Vertiefungsrichtung	Vertiefung Digitale Medien, Vertiefung Informatik und Software-Entwicklung
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
1. Einführung (Motivation, Begriffe, Projektphasen und Prozessmodelle) 2. Projektstart (Projektziele, Risiken in Softwareprojekten, Projektorganisation) 3. Projektplanung (Grundlagen der Projektplanung, Planungsreihenfolge, Planungstechniken) 4. Projektkontrolle (Voraussetzungen, Kontrollgrößen und Metriken) 5. Projektabschluss (Produktübergabe, Projektanalyse) 6. Teamführung (Motivationstheorien, Führungshinweise)

39 Rechnernetze Vertiefung

Computer Networks (Advanced Course)

Semester	Wahlpflichtbereich
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Wahlpflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Andreas Hanemann, Technische Hochschule Lübeck
Lerngebiet	Fachübergreifende Vertiefung (Informatik)
Teilnahmevoraussetzungen	empfohlen: Rechnernetze Grundlagen
Lernergebnisse	Die Studierenden sind in der Lage, anhand der Eigenschaften von Medien zu bewerten, ob der Einsatz eines bestimmten Mediums für einen vorgegebenen Zweck geeignet ist. Hierfür können sie auch die für den Zweck notwendigen Anforderungen bestimmen. Die Studierenden können festlegen, auf welche Weise die Wegewahlentscheidungen in einem Netzwerk getroffen werden sollen. Sie können dafür die geeigneten Komponenten (Switches, Router) auswählen und auch deren wesentliche Konfiguration angeben. Die Studierenden sind mit Virtualisierungskonzepten auf unterschiedlichen Ebenen (VLAN, MPLS, SDN) vertraut und können entscheiden, welche Art von Virtualisierung für ein gegebenes Netzwerk sinnvoll ist. Die Studierenden können eine geeignete Management-Lösung für ein vorgegebenes Netzwerk entwickeln bzw. anpassen. Dafür können sie entscheiden, welche Management-Informationen benötigt werden, wie diese erhoben werden sollen und wie die Auswertung erfolgen soll.
Prüfungsvorleistung	Einsendeaufgabe, Gruppenarbeit via Internet
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chat, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 130 h Webkonferenzteilnahme: ca. 12 h Präsenzteilnahme: 6 h Prüfung: 120 Minuten

Präsenzinhalte	In der ersten Präsenz werden Versuche mit Routern im Labor durchgeführt. In der zweiten Präsenz wird eine Aufgabensammlung zur Klausurvorbereitung besprochen.
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Kurose, James F.; Ross, Keith W. (2014): Computernetzwerke. Der Top-Down-Ansatz. 6., aktualisierte Auflage., Pearson Deutschland. Tanenbaum, Andrew S.; Wetherall, David (2012): Computernetzwerke. 5., aktualisierte Aufl., Pearson Deutschland.
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte

Netzzugang für Endnutzer
- Übertragungsmedien
- Analoge und digitale Signale
- Modulation
- Digitale Übertragung
- Leitungscodes
- Modems
- Digital Subscriber Line
- FTTx
- Kabelmodems
- Datenkommunikation über Stromnetze

Voice-over-IP
- Warum VoIP?
- Messverfahren
- Welche Protokolle werden benötigt?
- Real-Time Transport Protocol
- RTP Control Protocol
- Netzbelastung und Stauprobleme
- Portnummern VoIP
- RTP/RTCP Traces
- Session Initiation Protocol

Weitverkehrsnetze
- Aufbau von Weitverkehrsnetzen
- Open Shortest Path First (OSPF)
- Intermediate System to Intermediate System
- Border Gateway Protocol (BGP)
- Multiprotocol Label Switching

Campusnetze
- Aufbau von Campusnetzen

- Umgang mit Redundanz
- Virtualisierung
- Speichernetze
- Netze in der Gebäudeautomation

Netzwerk-Management
- Begriffe im Netzwerkmanagement
- Management nach OSI
- Simple Network Management Protocol (SNMP)
- Tools zum Netzwerk-Management
- Tools zum Netzwerk-Monitoring
- Einordnung in Prozessstandards

Netze in Automobilen
- Controller Area Network
- Local Interconnect Network
- FlexRay
- Media Oriented Systems Transport
- Automotive Ethernet

40 UNIX-basierte Betriebssysteme

UNIX-based Operating Systems

Semester	Wahlpflichtbereich
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Wahlpflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Dr. rer. nat. Ulrich Baum, Technische Hochschule Brandenburg
Lerngebiet	Fachübergreifende Vertiefung
Teilnahmevoraussetzungen	Empfohlen: Computerarchitektur und Betriebssysteme, Rechnernetze Grundlagen, Grundlagen der Programmierung 1 + 2
Lernergebnisse	Die Studierenden • sind mit den wesentlichen Konzepten und Begriffen Unix-basierter Betriebssysteme vertraut, • können ein Unix-basiertes Betriebssystem bedienen und administrieren, • kennen wichtige Programmierschnittstellen Unix-basierter Betriebssysteme und können diese in der Softwareentwicklung anwenden, • verstehen den grundsätzlichen Aufbau und die Arbeitsweise eines Unix/Linux-Kernels, • sind in der Lage, die Eignung verschiedener Unix-basierter Betriebssysteme für eine gegebene Anwendung zu beurteilen und mit anderen Betriebssystemen zu vergleichen.
Prüfungsvorleistung	keine
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chats, Webkonferenzen, Einsendeaufgaben u. a.) sowie Präsenzphasen. Praktische Übungen am eigenen Rechner unter Einsatz von virtuellen Maschinen und Cloud-Diensten.
Arbeitsaufwand	Selbststudium inkl. Erbringung der Prüfungsleistung: ca. 138 h Webkonferenzteilnahme: ca. 12 h
Prüfungsform	Portfolioprüfung
Literatur	Jain, Manish: Beginning Modern Unix, Apress, 2018. Kofler, Michael: Linux - Das umfassende Handbuch, 15. Aufl., Rheinwerk, 2017.

	Kroah-Hartman, Greg: Linux Kernel in a Nutshell, O´Reilly, 2006. Liu, Yukun, et. al., UNIX Operating System, Springer, 2011. Negus, Christopher: Linux Bible, 9th ed., Wiley, 2015. Nemeth, Evi et. al.: Unix and Linux System Administration Handbook, 5th ed., Pearson, 2017. Wang, K.C.: Systems Programming in Unix/Linux, Springer, 2018. Wolfinger, Christine: Keine Angst vor Linux/Unix, 11. Aufl., Springer Vieweg, 2013.
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten Unterrichtssprache ist auch Englisch.

Studieninhalte
Teil 1: Einführung, Bedienung, Administration • Überblick und historische Entwicklung • Wichtige Kommandozeilen-Befehle, Texteditor • Grundlagen der Shell-Programmierung • Netzwerke • Services • Systemadministration Teil 2: Unix-Konzepte und -Programmierschnittstelle am Beispiel von Linux • Prozesse und Threads • Scheduling • Interprozesskommunikation • Speicherverwaltung • Dateisysteme Teil 3: Aufbau und Arbeitsweise eines Unix-Kernels • Grundstruktur des Kernels • Labor mit einem für Lernzwecke entwickelten Unix-Kernel