MODULHANDBUCH

Master of Science

Master Cyber Security (FS-MACSD-60)

60 ECTS

Fernstudium

INTERNATIONALE HOCHSCHULE

Inhaltsverzeichnis

2022-05-01

1. Semester

IT Sicherheit und Datenschutz

Modulcode: DLMCSITSDS

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	keine	MA	5	150 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Ralf Kneuper (IT Sicherheit und Datenschutz)

Kurse im Modul

- IT Sicherheit und Datenschutz (DLMCSITSDS01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Fachpräsentation	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Datenschutz und Privatsphäre
- Bausteine der IT-Sicherheit
- IT-Sicherheitsmanagement
- Kryptographiekonzepte
- Kryptographie-Anwendungen

Qualifikationsziele des Moduls

IT Sicherheit und Datenschutz

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Kernkonzepte von IT-Sicherheit, Datenschutz und Kryptographie einschließlich ihrer Unterschiede und Beziehungen zu erklären.
- die Ansätze zum Datenschutz in verschiedenen Rechtsordnungen zu vergleichen.
- Datenschutzkonzepte auf die Datenwissenschaft und andere Anwendungsszenarien anzuwenden
- eine Analyse von Anwendungsszenarien durchzuführen, um die geeigneten Maßnahmen für das IT-Sicherheitsmanagement zu identifizieren, die umgesetzt werden sollten.
- Anwendungsszenarien zu untersuchen, um die geeigneten kryptografischen Konzepte zu identifizieren.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der IUBH**
Ist Grundlage für weitere Module im Bereich Informatik & Software-Entwicklung	Alle Master-Programme im Bereich IT & Technik

IT Sicherheit und Datenschutz

Kurscode: DLMCSITSDS01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		5	keine

Beschreibung des Kurses

Mit der zunehmenden Digitalisierung und Vernetzung von IT-Systemen ist der Bedarf gestiegen, Systeme und die von diesen Systemen verarbeiteten Daten zu schützen. Ziel dieses Moduls ist es, ein Verständnis für die erforderlichen Sicherheitsmaßnahmen, die IT-Sicherheit einschließlich Kryptographie und den Datenschutz zu vermitteln. Während der Bedarf an IT-Sicherheit weltweit ähnlich ist, haben verschiedene Kulturen unterschiedliche Erwartungen an Datenschutz und Privatsphäre. Dennoch werden personenbezogene Daten oft außerhalb des Landes verarbeitet, in dem die betroffenen Personen leben. Daher müssen die kulturellen Aspekte des Datenschutzes bei der Verarbeitung der Daten berücksichtigt werden. Dieser Kurs gibt einen Überblick über die wichtigsten IT-Sicherheitsmaßnahmen in verschiedenen Anwendungsszenarien sowie deren Integration in ein Informationssicherheitsmanagementsystem mit besonderem Fokus auf die relevante Normenfamilie ISO/IEC 270xx. Die Kryptographie stellt ein wichtiges Werkzeug für die IT-Sicherheit dar und wird in vielen verschiedenen Anwendungsszenarien wie sicheren Internetprotokollen und Block Chain eingesetzt.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Kernkonzepte von IT-Sicherheit, Datenschutz und Kryptographie einschließlich ihrer Unterschiede und Beziehungen zu erklären.
- die Ansätze zum Datenschutz in verschiedenen Rechtsordnungen zu vergleichen.
- Datenschutzkonzepte auf die Datenwissenschaft und andere Anwendungsszenarien anzuwenden
- eine Analyse von Anwendungsszenarien durchzuführen, um die geeigneten Maßnahmen für das IT-Sicherheitsmanagement zu identifizieren, die umgesetzt werden sollten.
- Anwendungsszenarien zu untersuchen, um die geeigneten kryptografischen Konzepte zu identifizieren.

Kursinhalt

1. Grundlagen von Datenschutz und IT-Sicherheit
   - 1.1 Terminologie und Risikomanagement
   - 1.2 Kernkonzepte der IT-Sicherheit
   - 1.3 Kernkonzepte von Datenschutz und Privatsphäre
   - 1.4 Kernkonzepte der Kryptografie
   - 1.5 Rechtliche Aspekte

2. Datenschutz
   - 2.1 Grundbegriffe des Datenschutzes (ISO/IEC 29100, Privacy by Design)
   - 2.2 Datenschutz in Europa: die DSGVO
   - 2.3 Datenschutz in den USA
   - 2.4 Datenschutz in Asien

3. Anwendung des Datenschutzes
   - 3.1 Anonymität und Pseudonyme
   - 3.2 Datenschutz in der Datenwissenschaft und Big Data
   - 3.3 Benutzer-Tracking im Online-Marketing
   - 3.4 Cloud Computing

4. Bestandteile der IT-Sicherheit
   - 4.1 Authentifizierung, Zugriffsverwaltung und -kontrolle
   - 4.2 Endgerätesicherheit
   - 4.3 IT-Sicherheit in Netzwerken
   - 4.4 Entwicklung sicherer IT-Systeme

5. IT-Sicherheitsmanagement
   - 5.1 Sicherheitsrichtlinien
   - 5.2 Sicherheits- und Risikoanalyse
   - 5.3 Die ISO 27000-Reihe
   - 5.4 IT-Sicherheit und IT-Governance
   - 5.5 Beispiel: IT-Sicherheit für Kreditkarten (PCI DSS)

6. Kryptografie
   - 6.1 Grundbegriffe der Kryptografie
   - 6.2 Symmetrische Kryptografie
   - 6.3 Asymmetrische Kryptografie
   - 6.4 Kryptografie mit elliptischer Kurve
   - 6.5 Hash-Funktionen
   - 6.6 Sicherer Datenaustausch

7. Kryptografische Anwendung
   - 7.1 Digitale Signaturen
   - 7.2 Sichere Internet-Protokolle
   - 7.3 Blockchain
   - 7.4 Elektronisches Geld

Literatur

Pflichtliteratur

Weiterführende Literatur

- Bowman, C. et al. (2015): The architecture of privacy. On engineering technologies that can deliver trustworthy safeguards. O'Reilly, Sebastopol, CA.
- Hintzbergen, J. et al. (2015): Foundations of information security (3rd ed.). Van Haren Publishing, Zaltbommel.
- ISO/IEC 29100 (2011): Information technology — Security techniques — Privacy framework. ISO. (URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip [Retrieved: 11.3.2020]).
- Paar, C./Pelzl, J. (2011). Understanding cryptography: A textbook for students and practitioners. Springer, Heidelberg.
- The Open Web Application Security Project (OWASP) (2005): A guide to building secure web applications and web services. OWASP. (URL: https://www.um.es/atica/documentos/OWASPGuide2.0.1.pdf [Retrieved: 11.3.2020]).

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Fachpräsentation

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Musterklausur	

Cyber Risk Assessment und Management

Modulcode: DLMCSECRAM_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	keine	MA	5	150 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Jesus Luna Garcia (Cyber Risk Assessment und Management)

Kurse im Modul

- Cyber Risk Assessment und Management (DLMCSECRAM01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Organisatorisches IT-Risikomanagement
- Messung der Cyber-Bedrohung
- Modellierung von Bedrohungen
- Standardisierung und Konformität
- Risikobewertung
- Die Cyber-resiliente Organisation

Qualifikationsziele des Moduls

Cyber Risk Assessment und Management

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- den Prozess der Angriffsmodellierung zu verstehen.
- die Auswirkungen eines Angriffes mit den entstehenden Kosten in Verbindung zu bringen.
- sogenannte Black Swan Events zu verstehen.
- den Einfluss des rechtlichen Rahmens auf Risiken und Kosten zu bewerten.
- zu verstehen, wie ein Unternehmen Entscheidungen auf der Grundlage von Risiken treffen muss.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der IUBH**
Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung	Alle Master-Programme aus dem Bereich IT & Technik

Cyber Risk Assessment und Management

Kurscode: DLMCSECRAM01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		5	keine

Beschreibung des Kurses

Entscheidungen darüber, ob Änderungen vorgenommen werden oder nicht, sollten in Abhängigkeit des Risikos der Auswirkungen eines Einschreitens oder Nicht-Einschreitens getroffen werden. Dies wird neben anderen Faktoren auch von den Kosten bestimmt, die ein potenziell erfolgreicher Angriff verursachen würde. Aber wie kann man Angriffe modellieren und die Kosten mit ihnen in Verbindung bringen? Wir werden uns in diesem Kurs mit der Disziplin der Angriffsmodellierung und Risikobewertung befassen.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- den Prozess der Angriffsmodellierung zu verstehen.
- die Auswirkungen eines Angriffes mit den entstehenden Kosten in Verbindung zu bringen.
- sogenannte Black Swan Events zu verstehen.
- den Einfluss des rechtlichen Rahmens auf Risiken und Kosten zu bewerten.
- zu verstehen, wie ein Unternehmen Entscheidungen auf der Grundlage von Risiken treffen muss.

Kursinhalt

1. Organisatorisches IT-Risikomanagement
   - 1.1 Geschäftlicher Nutzen von Risikomanagement
   - 1.2 Aufbau eines Angriffes zur Exfiltration von Daten
   - 1.3 Cyber-Katastrophen
   - 1.4 Cyber-Risiko

2. Messung der Cyber-Bedrohung
   - 2.1 Messung und Management
   - 2.2 Metriken zur Cyber-Bedrohung
   - 2.3 Messung der Bedrohung für eine Organisation
   - 2.4 Wahrscheinlichkeit schwerwiegender Cyber-Angriffe
   - 2.5 Black Swan Events

3. Modellierung von Bedrohungen
   - 3.1 Attack Tree-Methodik
   - 3.2 STRIDE
   - 3.3 DREAD
   - 3.4 LINDDUN

4. Standardisierung und Konformität
   - 4.1 NIST-Risikomanagement-System
   - 4.2 ISO 27005
   - 4.3 BSI 100-3

5. Risikobewertung
   - 5.1 Methodologien
   - 5.2 Systemische Betrachtung der Black Swan Events
   - 5.3 Kontinuierliche Neubewertung

6. Die Cyber-resiliente Organisation
   - 6.1 Veränderte Herangehensweisen an das Risikomanagement
   - 6.2 Reaktion auf Zwischenfälle und Krisenmanagement
   - 6.3 Resilience Engineering, Sicherheitslösungen und Finanzen
   - 6.4 Planung der Reaktion auf Zwischenfälle
   - 6.5 Cyber-Versicherung

Literatur

Pflichtliteratur

Weiterführende Literatur

- Allianz für Cyber-Sicherheit (2018): Management von Cyber-Risiken. Handbuch für Unternehmensvorstände und Aufsichtsräte. (URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/partner/20181004_Handbuch_Cyber_Risiken.html [letzter Zugriff: 01.03.2021]).
- Coburn, A./Leverett, E./Woo, G. (2018): Solving Cyber Risk. Protecting Your Company and Society. John Wiley & Sons, Hoboken, NJ.
- Joint Task Force Transformation Initiative (2012): Guide for Conducting Risk Assessments. Revision 1, NIST Computer Security Division. (URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final [Retrieved: 13.02.2021]).
- Königs, H. (2017): IT-Risikomanagement mit System. Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken. Springer-Verlag, Berlin.
- Pfleeger, C. P. (1996): Security in Computing. Prentice-Hall, Upper Saddle River, NJ.
- Schneier, B. (1999): Attack Trees. (URL: https://www.schneier.com/academic/archives/1999/12/attack_trees.html [Retrieved: 13.02.2021]).
- Shostack, A. (2014): Threat Modeling. Designing for Security. John Wiley & Sons, Hoboken, NJ.
- Wrede D. et al. (2018): Herausforderungen und Implikationen für das Cyber-Risikomanagement sowie die Versicherung von Cyberrisiken. Eine empirische Analyse. In: ZVersWiss, 107. Jg., S. 405–434.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Programmieren mit Python

Modulcode: DLMDWPMP

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	keine	MA	5	150 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Kamal Bhattacharya (Programmieren mit Python)

Kurse im Modul

- Programmieren mit Python (DLMDWPMP01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Schriftliche Ausarbeitung: Hausarbeit	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Einführung in die Programmiersprache Python
- Objektorientierte Konzepte in Python
- Behandlung von Ausnahmen und Fehlern
- Das Ökosystem der Python-Bibliothek
- Umgebungen und Paketmanagement
- Dokumentation und Prüfung
- Versionskontrolle

Qualifikationsziele des Moduls

Programmieren mit Python

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegende Python-Syntax und die Programmierkonzepte zu verstehen.
- sich an objektorientierte Konzepte in Python zu erinnern.
- verschiedene Methoden zur Fehlerbehandlung in Python zu analysieren und anzuwenden.
- gängige und wichtige Python-Bibliotheken zu kennen und wissen, wie man sie auf bestimmte Programmieraufgaben anwendet.
- Konzepte wie Umgebungen und Versionskontrolle zu verstehen .

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der IUBH**
Ist Grundlage für weitere Module im Bereich Data Science & Artificial Intelligence	Alle Master-Programme im Bereich IT & Technik

Programmieren mit Python

Kurscode: DLMDWPMP01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		5	keine

Beschreibung des Kurses

Python ist eine der vielseitigsten und am weitesten verbreiteten Skriptsprachen. Seine klare und übersichtliche Syntax sowie sein geradliniges Design tragen wesentlich zu diesem Erfolg bei und machen ihn zu einer idealen Sprache für die Programmierausbildung. Die Anwendungsgebiete reichen von der Webentwicklung bis hin zum wissenschaftlichen Rechnen. Insbesondere in den Bereichen Datenwissenschaft und künstliche Intelligenz ist sie die gebräuchlichste Programmiersprache, die von allen wichtigen Datenverarbeitungs- und Analyseframeworks unterstützt wird. Dieser Kurs bietet eine gründliche Einführung in die Sprache und ihre Hauptfunktionen sowie Einblicke in die Begründung und Anwendung wichtiger angrenzender Konzepte wie Umgebungen, Tests und Versionskontrolle.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die grundlegende Python-Syntax und die Programmierkonzepte zu verstehen.
- sich an objektorientierte Konzepte in Python zu erinnern.
- verschiedene Methoden zur Fehlerbehandlung in Python zu analysieren und anzuwenden.
- gängige und wichtige Python-Bibliotheken zu kennen und wissen, wie man sie auf bestimmte Programmieraufgaben anwendet.
- Konzepte wie Umgebungen und Versionskontrolle zu verstehen .

Kursinhalt

1. Einführung in Python
   - 1.1 Datenstrukturen
   - 1.2 Funktionen
   - 1.3 Durchflusskontrolle
   - 1.4 Eingang / Ausgang
   - 1.5 Module & Pakete

2. Klassen und Vererbung
   - 2.1 Bereiche und Namensräume
   - 2.2 Klassen und Vererbung
   - 2.3 Iteratoren und Generatoren

3. Fehler und Ausnahmen
   - 3.1 Syntaxfehler
   - 3.2 Behandlung und Auslösung von Ausnahmen
   - 3.3 Benutzerdefinierte Ausnahmen

4. Wichtige Bibliotheken
   - 4.1 Standard-Python-Bibliothek
   - 4.2 Wissenschaftliche Berechnungen
   - 4.3 Beschleunigung von Python
   - 4.4 Visualisierung
   - 4.5 Zugriff auf Datenbanken

5. Arbeiten mit Python
   - 5.1 Virtuelle Umgebungen
   - 5.2 Verwaltung von Paketen
   - 5.3 Unit- und Integrationstests
   - 5.4 Dokumentation des Codes

6. Versionskontrolle
   - 6.1 Einführung in die Versionskontrolle
   - 6.2 Versionskontrolle mit GIT

Literatur

Pflichtliteratur

Weiterführende Literatur

- Barry, P. (2016): Head first Python: A brain-friendly guide. 2nd edition, O'Reilly Publishing, Sebastopol, CA.
- Beazley, D. / Jones, B. K. (2013): Python cookbook. 3rd edition, O'Reilly Publishing, Sebastopol, CA.
- Lutz, M. (2013): Learning Python. O'Reilly Publishing, Sebastopol, CA.
- McKinney, W. (2017): Python for data analysis. 2nd edition, O'Reilly Publishing, Sebastopol, CA.
- Ramalho, L. (2015): Fluent Python: Clear, concise, and effective programming. O'Reilly Publishing, Sebastopol, CA.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Hausarbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Musterklausur	

DLMDWPMP01

Theoretische Informatik für IT-Sicherheit

Modulcode: DLMCSETCSITS_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	keine	MA	5	150 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Alexander Lawall (Theoretische Informatik für IT-Sicherheit)

Kurse im Modul

- Theoretische Informatik für IT-Sicherheit (DLMCSETCSITS01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Algorithmen und Datenstrukturen
- Formale Sprachen und Automatentheorie
- Berechenbarkeit, Entscheidbarkeit und Komplexität
- Logik
- Algorithmus- und Programmverifizierung
- Künstliche Intelligenz und Maschinelles Lernen

Qualifikationsziele des Moduls

Theoretische Informatik für IT-Sicherheit

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grenzen von Datenstrukturen, Algorithmen und Berechnungen im Allgemeinen zu verstehen.
- formale Sprachen und Automaten zur Lösung von Sicherheitsproblemen einzusetzen.
- Techniken des maschinellen Lernens bei der Datenanalyse einzusetzen.
- Logik und Wissensrepräsentation zu verwenden.
- die Prinzipien der Programmanalyse und –überprüfung zu verstehen.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der IUBH**
Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung	Alle Master-Programme aus dem Bereich IT & Technik

Theoretische Informatik für IT-Sicherheit

Kurscode: DLMCSETCSITS01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		5	keine

Beschreibung des Kurses

In der Praxis der IT-Sicherheit stoßen wir oft an die Grenzen der Informationstechnik und der Informatik. Was manchmal so aussieht, als sollte es lösbar sein, erweist sich für heutige Computer als schwierig oder unmöglich. Die Theoretische Informatik liefert den Rahmen für das Verständnis schwieriger Probleme und bietet oft einen Weg zu anderen Lösungen. Hier kann maschinelles Lernen oft eine stochastische Lösung bieten, wo es keine genaue gibt. Wir behandeln in diesem Kurs auch das Thema Programmanalyse und -verifikation.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grenzen von Datenstrukturen, Algorithmen und Berechnungen im Allgemeinen zu verstehen.
- formale Sprachen und Automaten zur Lösung von Sicherheitsproblemen einzusetzen.
- Techniken des maschinellen Lernens bei der Datenanalyse einzusetzen.
- Logik und Wissensrepräsentation zu verwenden.
- die Prinzipien der Programmanalyse und –überprüfung zu verstehen.

Kursinhalt

1. Algorithmen und Datenstrukturen
   - 1.1 Algorithmen, Programmiersprachen und Datenstrukturen
   - 1.2 Graphen und Bäume
   - 1.3 Sortieren und Suche
   - 1.4 Analyse von Algorithmen
2. Formale Sprachen und Automatentheorie
   - 2.1 Sprachen und Grammatiken
   - 2.2 Reguläre Sprachen und endliche Automaten
   - 2.3 Kontextfreie Sprachen und Kellerautomaten
   - 2.4 Kontextsensitive Sprachen und Turingmaschinen

3. Berechenbarkeit, Entscheidbarkeit und Komplexität
   - 3.1 Berechenbarkeit
   - 3.2 Entscheidbarkeit und Entscheidungsprobleme
   - 3.3 Komplexitätsheorie
   - 3.4 Quantencomputing

4. Logik
   - 4.1 Aussagenlogik
   - 4.2 Prädikatenlogik
   - 4.3 Resolutionskalkül
   - 4.4 Tableaukalkül

5. Algorithmus- und Programmverifizierung
   - 5.1 Programmanalyse
   - 5.2 Algebraische, operationale und denotationale Semantik
   - 5.3 Abstrakte Interpretation

6. Künstliche Intelligenz und Maschinelles Lernen
   - 6.1 Überwachtes vs. unüberwachtes Lernen
   - 6.2 Lineare und nichtlineare Regression
   - 6.3 Logistische Regression
   - 6.4 Künstliche Neuronale Netze

Literatur

Pflichtliteratur

Weiterführende Literatur

- Goodfellow, I. / Bengio, Y. / Courville, A. (2016): Deep Learning. MIT Press, Cambridge, MA.
- Graham, R. L. / Knuth, D. E. / Patashnik, O. (1994): Concrete Mathematics. A Foundation for Computer Science. 2nd Edition, Addison-Wesley, Upper Saddle River, NJ.
- Hoffmann, D. W. (2018): Theoretische Informatik. 4., aktualisierte Auflage, Carl Hanser Verlag GmbH & Co. KG, München.
- Hopcroft, J. E. / Ullman J. D. (2006): Introduction to Automata Theory, Languages, and Computation. 3rd Edition, Pearson Education, London.
- Kastens, U./Kleine Büning, H. (2018): Modellierung. Grundlagen und formale Methoden. 4., erweiterte Auflage. Carl Hanser Verlag GmbH & Co. KG, München.
- Krumke, S. O./Noltemeier, H. (2012): Graphentheoretische Konzepte und Algorithmen. 3. Auflage, Vieweg+Teubner Verlag, Wiesbaden.
- Nielson, F. / Nielson, H. R. / Hankin, C. (1999): Principles of Program Analysis. Springer, Berlin.
- Nipkow T. / Klein, G. (2016): Concrete Semantics. With Isabelle/HOL. Springer, Berlin.
- Russell, S. / Norvig, P. (2016): Artificial Intelligence. A Modern Approach. Pearson Education, London.
- Shaffer, C. A. (2011): Data Structures and Algorithm Analysis in C++. 3rd Edition, Dover Books on Computer Science, Mineola, NY.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Forschungsmethodik

Modulcode: DLMMET-01

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	keine	MA	5	150 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Julia Pitters (Forschungsmethodik)

Kurse im Modul

- Forschungsmethodik (MMET01-01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Kombistudium Klausur, 90 Minuten Studienformat: Fernstudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Einführung in Wissenschaftstheorien
- Voraussetzungen für quantitatives Messen und Testen
- Grundlagen der qualitativen Forschung

Qualifikationsziele des Moduls

Forschungsmethodik

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- unterschiedliche Annahmen und Herangehensweisen qualitativer und quantitativer Forschung zu kategorisieren.
- die methodologischen Voraussetzungen zu bestimmen, die bei der quantitativen Messung und Testung spezifischer Konstrukte gegeben sein müssen.
- die jeweiligen quantitativen Skalen und Indikatoren zielgerichtet in eigener Forschung einzusetzen.
- verschiedene qualitative Erhebungs- und Auswertungsverfahren voneinander zu differenzieren und in eigener Forschung anzuwenden.
- spezielle Probleme bei der Durchführung von Forschungsstudien zu analysieren und kennen diesbezügliche Lösungsmöglichkeiten, um eine optimale Durchführung von Forschung realisieren zu können.
- die Qualität von Forschungsvorhaben hinsichtlich quantitativer und qualitativer Gütekriterien bewerten zu können.
- Konzeptionen der Forschung im Hinblick auf Forschungsphilosophie, Forschungsansatz und ethischen Aspekten zu bewerten.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der IUBH**
Ist Grundlage für alle weiteren Module im Bereich Methoden.	Alle Master-Programme im Bereich Wirtschaft & Management

Forschungsmethodik

Kurscode: MMET01-01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		5	keine

Beschreibung des Kurses

Der Kurs vermittelt in kritischer Weise zuerst den wissenschaftstheoretischen Hintergrund und die Terminologie der entsprechenden forschungstheoretischen Paradigmen, um den Studierenden die unterschiedliche Herangehensweise qualitativer und quantitativer Methodik verständlich zu machen. Dabei werden die unterschiedlichen Perspektiven der Wissenschaftstheorie in die Betrachtung einbezogen.Aufbauend auf die Skalenniveaus, lernen die Studierenden die Annahmen der klassischen sowie der probabilistischen Testtheorie kennen, um auf deren Basis die Anforderungen an Forschungsmethoden im Sinne der Qualitätskriterien sowie die Notwendigkeit der Bildung verschiedener Skalentypen und Indikatoren nachvollziehen zu können.Die wichtigen Aspekte der Konzeption der Forschung, ausgehend von der Forschungsphilosophie bis hin zu ethischen Dimensionen der Forschung werden verknüpft mit der Betrachtung von quantitativer und qualitativer Forschung um letztendlich deren Verbindung der Triangulation aufzuzeigen. Wichtig bei den Untersuchungsdesigns ist es, deren Güte in der Umsetzung festzustellen, sodass Gütekriterien sowohl bei qualitativer als auch bei quantitativer Forschung im Fokus stehen. Den Abschluss bilden Methoden der Datengenerierung und Methoden der Datenanalyse von qualitativer Forschung. Dabei werden die bedeutsamen Methoden der Datenanalyse wie die Inhaltsanalyse, Grounded Theorie und die Diskursanalyse sowohl theoretisch als auch praxisorientiert näher gebracht und den Studierenden die Möglichkeit eingeräumt, besondere Interviewformen – wie das fokussierte Interview oder das narrative Interview – neben der theoretischen Beschäftigung auch in der konkreten Umsetzung wahrzunehmen, aber auch Beobachtung und Feldnotizen zu betrachten.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- unterschiedliche Annahmen und Herangehensweisen qualitativer und quantitativer Forschung zu kategorisieren.
- die methodologischen Voraussetzungen zu bestimmen, die bei der quantitativen Messung und Testung spezifischer Konstrukte gegeben sein müssen.
- die jeweiligen quantitativen Skalen und Indikatoren zielgerichtet in eigener Forschung einzusetzen.
- verschiedene qualitative Erhebungs- und Auswertungsverfahren voneinander zu differenzieren und in eigener Forschung anzuwenden.
- spezielle Probleme bei der Durchführung von Forschungsstudien zu analysieren und kennen diesbezügliche Lösungsmöglichkeiten, um eine optimale Durchführung von Forschung realisieren zu können.
- die Qualität von Forschungsvorhaben hinsichtlich quantitativer und qualitativer Gütekriterien bewerten zu können.
- Konzeptionen der Forschung im Hinblick auf Forschungsphilosophie, Forschungsansatz und ethischen Aspekten zu bewerten.

Kursinhalt

1. Wissenschaftliche Grundlagen
   - 1.1 Grundlegende Vorstellungen in der Wissenschaft
   - 1.2 Von der Idee zum Forschungsvorhaben
   - 1.3 Erklärungsansätze in der Wissenschaft
2. Perspektiven in der Wissenschaftstheorie
   - 2.1 Vom logischen Empirismus zum kritischen Rationalismus
   - 2.2 Konstruktivismus
   - 2.3 Methodischer Anarchismus
3. Quantitatives Messen mit der klassischen und probabilistischen Testtheorie
   - 3.1 Skalenniveaus und die Unterscheidung manifester und latenter Merkmale
   - 3.2 Klassische Testtheorie
   - 3.3 Probabilistische Testtheorie
4. Grundlegende Konzepte der Itembildung
   - 4.1 Skalierungsverfahren
   - 4.2 Indexbildung
5. Konzeption der Forschung
   - 5.1 Wissenschaftstheorie und Forschungsprozess
   - 5.2 Ethische Aspekte der Forschung – Forschungsethik

6. Untersuchungsdesign
   - 6.1 Der qualitative und der quantitative Ansatz
   - 6.2 Die Dichtonomie von „quantitativ versus qualitativ“ – eine Begriffsbestimmung

7. Prüfung der Gütekriterien in der quantitativen und qualitativen Forschung
   - 7.1 Das Gütekriterium Objektivität
   - 7.2 Das Gütekriterium Reliabilität
   - 7.3 Das Gütekriterium Validität

8. Durchführen qualitativer Forschung
   - 8.1 Methoden der Datengenerierung
   - 8.2 Besondere Interviewformen

9. Methoden der qualitativen Analyse
   - 9.1 Inhaltsanalyse
   - 9.2 Grounded Theory
   - 9.3 Diskursanalyse

Literatur

Pflichtliteratur

Weiterführende Literatur

- Bortz, J./Döring, N. (2006): Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler. 4. Auflage, Springer, Heidelberg.
- Diekmann, A. (2007): Empirische Sozialforschung. Grundlagen, Methoden, Anwendungen. 4. Auflage, Rowohlt, Reinbek.
- Kromrey, H. (2009): Empirische Sozialforschung. 12. Auflage, UTB, Stuttgart.
- Lamnek, S. (2010): Qualitative Sozialforschung. 5. Auflage, Beltz, Weinheim.
- Mayring, P. (2002): Einführung in die Qualitative Sozialforschung. 5. Auflage, Beltz, Weinheim.
- Mayring, P. (2010): Qualitative Inhaltsanalyse. Grundlagen und Techniken. 11. Auflage, Beltz, Weinheim.
- Schnell, R./Hill, P. B./Esser, E. (2008): Methoden der empirischen Sozialforschung. 8. Auflage, Oldenbourg, München.
- Sedlmeier, P./Renkewitz, F. (2007): Forschungsmethoden und Statistik in der Psychologie. Pearson Studium, München.

Studienformat Kombistudium

Studienform	**Kursart**
Kombistudium	Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden	
☐ Learning Sprints®	☑ Repetitorium
☑ Skript	☐ Creative Lab
☑ Vodcast	☐ Prüfungsleitfaden
☐ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden	
☐ Learning Sprints®	☑ Repetitorium
☑ Skript	☐ Creative Lab
☑ Vodcast	☐ Prüfungsleitfaden
☐ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Cybersysteme und Netzwerkforensik

Modulcode: DLMCSECSNF_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	keine	MA	5	150 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Alexander Lawall (Cybersysteme und Netzwerkforensik)

Kurse im Modul

- Cybersysteme und Netzwerkforensik (DLMCSECSNF01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Klausur, 90 Minuten	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Betriebssysteme
- Vernetzung
- Forensik
- Kryptographie
- Cyber-Angriffe

Qualifikationsziele des Moduls

Cybersysteme und Netzwerkforensik

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- grundlegende interne Strukturen, Aufbau und Funktionen von Betriebssystemen zu verstehen.
- die wichtigsten Netzwerkprotokolle zu verstehen.
- Angriffe auf Computer und Netzwerke zu diagnostizieren
- die Wichtigkeit der Beweiserhebung und Beweissicherung zu verstehen.
- wesentliche Angriffsmuster zu verstehen.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der IUBH**
Ist Grundlage für alle weiteren Module aus dem Bereich Informatik & Software-Entwicklung	Alle Master-Programme aus dem Bereich IT & Technik

Cybersysteme und Netzwerkforensik

Kurscode: DLMCSECSNF01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		5	keine

Beschreibung des Kurses

Der Computersicherheitsexperte hat die schwierige Aufgabe, sowohl die Grundlagen von Betriebssystemen als auch von Netzwerken kennen zu müssen. In diesem Kurs betrachten wir Betriebssysteme und Netzwerke aus forensischer Sicht. Das Endergebnis ist das Verständnis von Angriffen auf eine Organisation.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- grundlegende interne Strukturen, Aufbau und Funktionen von Betriebssystemen zu verstehen.
- die wichtigsten Netzwerkprotokolle zu verstehen.
- Angriffe auf Computer und Netzwerke zu diagnostizieren
- die Wichtigkeit der Beweiserhebung und Beweissicherung zu verstehen.
- wesentliche Angriffsmuster zu verstehen.

Kursinhalt

1. Betriebssysteme
   - 1.1 Konzepte
   - 1.2 Speicherverwaltung
   - 1.3 Prozess-Management
   - 1.4 Geräteverwaltung
   - 1.5 Eingabe/Ausgabe
2. Betriebssystembausteine
   - 2.1 Systemaufraufe
   - 2.2 Prozesstabellen-Analyse
   - 2.3 Windows-Registrierungsdatenbank
   - 2.4 Dateisystem-Forensik
   - 2.5 Typische Angriffe

3. Der Netzwerkstapel
   - 3.1 TCP/IP- und OSI-Netzwerkstapel
   - 3.2 Zentrale Internet-Dienste
   - 3.3 Das World Wide Web
   - 3.4 Transportschicht-Verschlüsselung
   - 3.5 Typische Angriffe

4. Computer-Forensik
   - 4.1 Beweisführung
   - 4.2 Schadsoftware
   - 4.3 Daten-Exfiltration
   - 4.4 Angriffe gegen Computer-Forensik

5. Netzwerk-Forensik
   - 5.1 Indikatoren für eine Kompromittierung
   - 5.2 Einbindung externer Daten (Datenanreicherung) und Entscheidungspunkte
   - 5.3 Angriffe gegen die Netzwerk-Forensik

6. Angriffe aus der Sicht des Zentralrechners und des Netzwerks
   - 6.1 Techniken, Taktiken und Verfahren
   - 6.2 Erkennung und Verhinderung von Eindringversuchen
   - 6.3 Korrelation von Ereignissen

Literatur

Pflichtliteratur

Weiterführende Literatur

- Kaufman C. / Perlman, R. / Speciner, M. (2002): Network Security: Private Communication in a Public World, Second Edition, Pearson Education, London.
- Oorschot, P. C. (2020): Computer Security and the Internet. Springer Nature, Berlin.
- Pfleeger C. P. / Pfleeger S. L. / Marguilies, J. (2015): Security in Computing. 5th Edition, Pearson Education, London.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

DLMCSECSNF01_D

2. Semester

Seminar: Standards und Frameworks

Modulcode: DLMIMSSF

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	keine	MA	5	150 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. André Köhler (Seminar: Standards und Frameworks)

Kurse im Modul

- Seminar: Standards und Frameworks (DLMIMSSF01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
Studienformat: Fernstudium Schriftliche Ausarbeitung: Seminararbeit	

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

- Das Seminar stellt eine Methodik vor, um Prinzipien von Standards und Rahmenwerken zu hinterfragen, explizite und implizite Annahmen zu identifizieren und zu validieren und empfohlene Kategorisierungen und Arbeitsabläufe hinsichtlich ihrer Umsetzbarkeit zu bewerten.

Qualifikationsziele des Moduls

Seminar: Standards und Frameworks

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- IT-relevante Standards und Frameworks zu benennen und anhand derer Einsatzgebiete abzugrenzen.
- Prinzipien der Standards und Frameworks auf ihre Umsetzbarkeit und logische Argumentation hin zu hinterfragen.
- gemachte Annahmen in Standards zu identifizieren und zu validieren.
- empfohlene Kategorisierungen und Arbeitsabläufe auf ihre Plausibilität hin zu überprüfen.
- administrative und technische Voraussetzungen für die Implementierung zu identifizieren.
- Erwartungen der Stakeholder zu identifizieren und zu priorisieren.
- Empfehlungen zur Umsetzung und Erhaltung der Standards zu geben.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der IUBH**
Ist Grundlage für weitere Module im Bereich Informatik & Software-Entwicklung	Alle Master-Programme im Bereich IT & Technik

Seminar: Standards und Frameworks

Kurscode: DLMIMSSF01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		5	keine

Beschreibung des Kurses

Das Seminar macht Studierende mit einer Vorgehensweise zur kritischen Beurteilung internationaler Standards und Rahmenwerke der IT vertraut. Studierende werden damit in die Lage versetzt, in einem gegebenen Industrieszenario die Nutzbarkeit und Grenzen eines Standards einzuschätzen und Entscheidungsträgern entsprechende Empfehlungen zu geben.Das Seminar fokussiert dabei auf die kritische Beurteilung der Prinzipien und Annahmen der Standards, der Konsistenz und Kohärenz empfohlener Kategorien und Arbeitsanweisungen und der Einschätzung der Umsetzbarkeit, Implementierung und Erhaltung des Standards.Auf dieser Basis erstellen die Studierenden für einen gegebenen Standard in einem gegebenen Industrieszenario einen Bericht, der den Standard entsprechend dieser Kriterien bewertet und mit einer Empfehlung zur Befürwortung oder Ablehnung des Standards abschließt.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- IT-relevante Standards und Frameworks zu benennen und anhand derer Einsatzgebiete abzugrenzen.
- Prinzipien der Standards und Frameworks auf ihre Umsetzbarkeit und logische Argumentation hin zu hinterfragen.
- gemachte Annahmen in Standards zu identifizieren und zu validieren.
- empfohlene Kategorisierungen und Arbeitsabläufe auf ihre Plausibilität hin zu überprüfen.
- administrative und technische Voraussetzungen für die Implementierung zu identifizieren.
- Erwartungen der Stakeholder zu identifizieren und zu priorisieren.
- Empfehlungen zur Umsetzung und Erhaltung der Standards zu geben.

Kursinhalt

- In diesem Kurs werden internationale Standards für den IT-Bereich auf ihre Nutzbarkeit und Voraussetzungen hin überprüft. Die gewählten Standards schließen de facto und de jure Standards, Good Practices (GxPs), Rahmenwerke (wie etwa ARIS, TOGAF, COBIT, ITIL, CMMI), Projektmanagement-Frameworks und diverse IT-relevante ISO-Standards ein.
  Die Analyse beginnt mit der Bewertung der Ähnlichkeiten und Unterschiede bezüglich der Einsatzgebiete der Standards. Darauf folgt eine Einschätzung der Intention der Herausgeber, der Popularität des Standards sowie der Begründung der Einführung in ausgewählten Industriesektoren. Auf dieser Basis erstellen die Studierenden eine Seminararbeit, in der sie

für einen gegebenen Standard in einem gegebenen Industrieszenario eine kritische Einschätzung der Umsetzbarkeit vornehmen. Die Seminararbeit deckt dabei folgende Kriterien ab:

- Prinzipien: Eine kritische Bewertung der Prinzipien des Standards für das gegebene Industrieszenario.
- Annahmen: Identifizierung der im Standard gemachten expliziten und impliziten Annahmen und deren Plausibilitätsprüfung im gegebenen Industrieszenario.
- Kategorien: Bewertung der Übereinstimmung der vorgegebenen Kategorisierungen mit dem Industrieszenario.
- Abläufe: Ermittlung der notwendigen Arbeitsabläufe und Einschätzung der Machbarkeit.
- Erwartungen: Identifizierung der Anforderungen und Erwartungen der Stakeholder.
- Konsistenzprüfung: Identifizierung von Widersprüchen in einer der vorgenannten Kategorien.
- Kohärenzprüfung: Bewertung der Vollständigkeit und ggf. Empfehlungen für weitere Standardisierung.
- Voraussetzungen: Ermittlung der Voraussetzungen zur Implementierung des Standards.
- Aufrechterhaltung: Eine Einschätzung des Aufwands zur Erhaltung und Pflege des Standards.

Die Seminararbeit schließt entweder mit einer Befürwortung oder einer Ablehnung des Standards für das gegebene Industrieszenario ab, die jeweils mit den Ergebnissen der Analyse rational begründet wird.

Literatur

Pflichtliteratur

Weiterführende Literatur

- Johannsen, W./Goeken, M. (2011): Referenzmodelle für IT-Governance. Methodische Unterstützung der Unternehmens-IT mit COBIT, ITIL & Co. dpunkt.verlag, Heidelberg.
- Krallmann, H./Bobrik, A./Levina, O. (Hrsg.) (2013): Systemanalyse im Unternehmen. Prozessorientierte Methoden der Wirtschaftsinformatik. Walter de Gruyter, Berlin.
- Müller, K. R. (2018): IT-Sicherheit mit System. Integratives IT-Sicherheits-, Kontinuitäts-und Risikomanagement–Sichere Anwendungen–Standards und Practices. Springer, Berlin.
- Rüter, A. et al. (Hrsg.) (2010): IT-Governance in der Praxis. Erfolgreiche Positionierung der IT im Unternehmen. Anleitung zur erfolgreichen Umsetzung regulatorischer und wettbewerbsbedingter Anforderungen. Springer, Berlin.
- Tiemeyer, E. (Hrsg.) (2016): Handbuch IT-Systemmanagement. Handlungsfelder, Prozesse, Managementinstrumente, Good-Practices. Carl Hanser Verlag, München.
- van Wessel, R. (Hrsg.) (2010): Toward Corporate IT Standardization Management. Frameworks and Solutions. IGI Global, Hershey, PA.
- Wagner, K. P. (2015): Ermittlung des Reifegrads von Informationstechnologie in kleinen und mittleren Unternehmen. Berliner Wissenschaftsverlag, Berlin.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Seminar

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Seminararbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

DLMIMSSF01

Steuerungsprozesse

Modulcode: DLMCSDWSP_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	keine	MA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. André Köhler (Management von IT-Projekten) / Prof. Dr. André Köhler (IT-Servicemanagement I)

Kurse im Modul

- Management von IT-Projekten (MWIT01)
- IT-Servicemanagement I (DLMIWSM01)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Management von IT-Projekten • Studienformat "Fernstudium": Klausur, 90 Minuten IT-Servicemanagement I • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Fallstudie

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Management von IT-Projekten

- Grundprinzipien und Aufgaben im IT-Projektmanagement
- SW-Lebenszyklus: Von Planung bis Ablösung
- Rollen, deren typische Aktivitäten sowie Schnittstellen zu anderen Rollen
- Phasen im SW-Prozess, sowie beteiligte Rollen, typische Aktivitäten
- Vorgehensmodelle bei der SW-Entwicklung
- Agile Management- und –Kommunikationstechniken

IT-Servicemanagement I

- Grundlagen und Begriffe zum IT-Servicemanagement
- IT Infrastructure Library (ITIL)
- ITIL – Service Design
- ITIL – Service Transition
- ITIL – Service Operation
- Information Security Management mit dem IT-Grundschutz-Framework des BSI

Qualifikationsziele des Moduls

Management von IT-Projekten

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- den Wissensstand über IT-Projektmanagement kritisch widerzuspiegeln.
- verschiedene IT-Projektmanagementformate (kleine, mittlere und große Projekte) aufzustellen und die Methoden zur professionellen Durchführung dieser verschiedenen IT-Projekte zu kennen.
- ein IT-Management-Angebots als Grundlage für ein professionelles IT-Projektmanagement-Konzept zu erstellen.
- verschiedene IT-Management-Projektpläne (z.B. Zeit-, Kosten-, Ressourcen- und Risikoplan) zu verstehen und zu integrieren und diese Pläne in einem integrativen IT-Projektplanungs- und Controllingsystem zu verwenden.
- ein IT-Projektteam und seine Kern- und/oder erweiterten Teammitglieder zu organisieren und anzuleiten.

IT-Servicemanagement I

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundlagen und Herausforderungen des IT-Servicemanagements zu kennen.
- die Motivation und den Aufbau der IT Infrastructure Library (ITIL) zu erkennen, die Hauptelemente zu beschreiben und konkrete Aktivitäten im Service Livecycle zu verorten.
- die Aktivitäten der ITIL-Governance und ITIL-Operational-Prozesse zu beschreiben, voneinander abzugrenzen und konkrete Lösungen unter Anwendung der Aktivitäten zu erarbeiten.

Bezüge zu anderen Modulen im Studiengang	Bezüge zu anderen Studiengängen der IUBH
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Master-Programme im Bereich IT & Technik

Management von IT-Projekten

Kurscode: MWIT01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		5	keine

Beschreibung des Kurses

Ziel dieses Kurses ist es, die Teilnehmer mit den Konzepten des IT-Projektmanagements vertraut zu machen. Dies wird durch die Entwicklung eines Verständnisses der grundlegenden Prinzipien des Projektmanagements erreicht, das die Fähigkeit der Studenten verbessert, ihre Kenntnisse, Fähigkeiten und Kompetenzen bei der Analyse und Lösung von IT-Projektmanagementproblemen anzuwenden. Ein besonderer Fokus liegt auf den Besonderheiten der IT-Projektorganisation, des Kostenmanagements und des Faktors Mensch in IT-Projekten.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- den Wissensstand über IT-Projektmanagement kritisch widerzuspiegeln.
- verschiedene IT-Projektmanagementformate (kleine, mittlere und große Projekte) aufzustellen und die Methoden zur professionellen Durchführung dieser verschiedenen IT-Projekte zu kennen.
- ein IT-Management-Angebots als Grundlage für ein professionelles IT-Projektmanagement-Konzept zu erstellen.
- verschiedene IT-Management-Projektpläne (z.B. Zeit-, Kosten-, Ressourcen- und Risikoplan) zu verstehen und zu integrieren und diese Pläne in einem integrativen IT-Projektplanungs- und Controllingsystem zu verwenden.
- ein IT-Projektteam und seine Kern- und/oder erweiterten Teammitglieder zu organisieren und anzuleiten.

Kursinhalt

1. Einführung: Merkmale von IT-Projekten
   - 1.1 Definition von IT-Projekten
   - 1.2 Überblick über typische Rollen und Phasen von IT-Projekten
   - 1.3 Risiken und Herausforderungen von IT-Projekten
   - 1.4 Rolle eines IT-Projektmanagers
2. Organisation der Arbeit
   - 2.1 Projektstrukturplan, Arbeitspakete
   - 2.2 Priorisierung
   - 2.3 Zeitplanung, Meilensteine, Gantt-Diagramm
   - 2.4 Definition des Erledigten

3. Kostenschätzung und Controlling
   - 3.1 Herausforderungen der Kostenschätzung in IT-Projekten
   - 3.2 Schätzverfahren: 3-Punkte-Schätzung, doppelte blinde Expertenschätzung, Funktionspunkte
   - 3.3 Kostenkontrolle mit Hilfe der Fortschrittsanalyse
   - 3.4 Risikomanagement

4. Der menschliche Faktor
   - 4.1 Visionserhaltung
   - 4.2 Stakeholder-Management
   - 4.3 Konfliktmanagement

5. Organisation von kleinen und mittleren Projekten
   - 5.1 Rational Unified Process (RUP)
   - 5.2 Agile Software-Prozesse
   - 5.3 Scrum
   - 5.4 Plangetriebenes Projektmanagement in kleinen Projekten

6. Organisation von Großprojekten
   - 6.1 PMBOK Leitfaden
   - 6.2 Prinz2
   - 6.3 Multi-Projektmanagement
   - 6.4 Agile Softwareprozesse in Großprojekten
   - 6.5 Auswahl der geeigneten Projektmanagementmethode

Literatur

Pflichtliteratur

Weiterführende Literatur

- Hinde, D. (2012): PRINCE2 Study Guide. John Wiley & Sons, West Sussex.
- Kneuper, R. (2018): Software processes and lifecycle models. Springer Nature, Cham.
- Phillips, J. (2010): IT project management: On track from start to finish. 3rd edition, McGraw-Hill, New York, NY.
- Project Management Institute. (2013): A guide to the project management body of knowledge: PMBOK guide.
- Schwaber, K. (2004): Agile project management with Scrum. Microsoft Press, Redmond, WA.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

IT-Servicemanagement I

Kurscode: DLMIWSM01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		5	keine

Beschreibung des Kurses

IT-Servicemanagement ist ein Ansatz, die IT eines Unternehmens als Dienstleister und Unterstützer der betrieblichen und geschäftlichen Prozesse auszurichten und zu verstehen. Hierbei stehen Qualitätsmanagement und Handhabung des täglichen Betriebs im Vordergrund.Dieser Kurs vermittelt unter Verwendung der IT Infrastructure Library (ITIL) Konzepte, Vorgehensweisen und Best-Practices im Bereich IT-Servicemanagement (IT-Betrieb). Damit werden also die Steuerung der Aktivitäten eines SW-Lebenszyklus betrachtet, die nach der Entwicklung eines IT-Systems stattfinden: der IT-Betrieb als kontinuierlichen Lauf des produktiven Tagesgeschäfts der IT-Abteilungen eines Unternehmens.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- die Grundlagen und Herausforderungen des IT-Servicemanagements zu kennen.
- die Motivation und den Aufbau der IT Infrastructure Library (ITIL) zu erkennen, die Hauptelemente zu beschreiben und konkrete Aktivitäten im Service Livecycle zu verorten.
- die Aktivitäten der ITIL-Governance und ITIL-Operational-Prozesse zu beschreiben, voneinander abzugrenzen und konkrete Lösungen unter Anwendung der Aktivitäten zu erarbeiten.

Kursinhalt

1. Grundlagen und Begriffe zum IT-Service Management
   - 1.1 IT-Dienstleistungen (auch: IT-Services, engl. IT services)
   - 1.2 IT-Servicemanagement
2. IT Infrastructure Library (ITIL)
   - 2.1 Service Livecycle und Prozessgruppen in ITIL
   - 2.2 Service Strategy
   - 2.3 Continual Service Improvement

3. ITIL – Service Design
   - 3.1 Service Level Management
   - 3.2 Service Catalog Management
   - 3.3 Availability Management
   - 3.4 Weitere Prozesse im Service Design

4. ITIL – Service Transition
   - 4.1 Transition Planning and Support
   - 4.2 Change Management
   - 4.3 Service Asset and Configuration Management (SACM)
   - 4.4 Weitere Prozesse in der Service Transition

5. ITIL – Service Operation
   - 5.1 Eventmanagement
   - 5.2 Incident Management
   - 5.3 Problemmanagement
   - 5.4 Weitere Prozesse in der Service Operation

6. Information Security Management mit dem IT-Grundschutz Framework des BSI
   - 6.1 Aufbau und Elemente des BSI-Grundschutzes
   - 6.2 Informationssicherheitsprozess

Literatur

Pflichtliteratur

Weiterführende Literatur

- Beims, M. (2012): IT-Service Management in der Praxis mit ITIL. Hanser, München.
- Renner, B./Moser, U./Schmid, D. (2006): IT-Service-Management. Transparente IT-Leistungen & Messbare Qualität. BPX Edition, Rheinfelden.
- Tiemeyer, E. (Hrsg.) (2011): Handbuch IT-Management. Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis. Hanser, München.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Fallstudie

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Fallstudie

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
110 h	0 h	20 h	20 h	0 h	150 h

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☐ Musterklausur	

Künstliche Intelligenz

Modulcode: DLMIMWKI_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	keine	MA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Prof. Dr. Ulrich Kerzel (Künstliche Intelligenz) / Prof. Dr. Tim Schlippe (Seminar: Künstliche Intelligenz und Gesellschaft)

Kurse im Modul

- Künstliche Intelligenz (DLMAIAI01_D)
- Seminar: Künstliche Intelligenz und Gesellschaft (DLMAISAIS01_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Künstliche Intelligenz • Studienformat "Fernstudium": Klausur Seminar: Künstliche Intelligenz und Gesellschaft • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Seminararbeit

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Künstliche Intelligenz

- Geschichte der KI
- KI-Anwendungsbereiche
- Expertensysteme
- Neurowissenschaften
- Moderne KI-Systeme

Seminar: Künstliche Intelligenz und Gesellschaft

In diesem Seminar werden die Studierenden über die aktuellen gesellschaftlichen und politischen Implikationen der künstlichen Intelligenz nachdenken. Zu diesem Zweck werden relevante Themen in Form von Artikeln vorgestellt, die von den Studierenden in einem schriftlichen Aufsatz kritisch bewertet werden.

Qualifikationsziele des Moduls

Künstliche Intelligenz

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- sich einen Überblick über die historischen Entwicklungen im Bereich der künstlichen Intelligenz zu verschaffen.
- die verschiedenen Anwendungsbereiche der künstlichen Intelligenz zu analysieren.
- Expertensysteme zu verstehen.
- Prolog auf einfache Expertensysteme anzuwenden.
- das Gehirn und die kognitiven Prozesse aus neurowissenschaftlicher Sicht zu verstehen.
- moderne Entwicklungen in der künstlichen Intelligenz zu verstehen.

Seminar: Künstliche Intelligenz und Gesellschaft

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ausgewählte aktuelle gesellschaftliche Themen und Fragestellungen der künstlichen Intelligenz zu nennen.
- den Einfluss und die Auswirkungen der künstlichen Intelligenz auf gesellschaftliche, wirtschaftliche und politische Themen zu erklären.
- theoretisch erworbenes Wissen auf reale Fälle zu übertragen.
- ein ausgewähltes Thema in Form eines schriftlichen Aufsatzes wissenschaftlich zu behandeln.
- aktuelle gesellschaftliche und politische Fragen, die sich aus den jüngsten Fortschritten in der Methodik der künstlichen Intelligenz ergeben, kritisch zu hinterfragen und zu diskutieren.
- eigene Problemlösungsfähigkeiten und -prozesse durch Reflexion über die möglichen Auswirkungen ihrer zukünftigen Tätigkeit im Bereich der künstlichen Intelligenz zu entwickeln.

Bezüge zu anderen Modulen im Studiengang	Bezüge zu anderen Studiengängen der IUBH
Baut auf Modulen aus dem Bereich Data Science & Artificial Intelligence auf	Alle Master-Programme im Bereich IT & Technik

Künstliche Intelligenz

Kurscode: DLMAIAI01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		5	keine

Beschreibung des Kurses

Die Suche nach künstlicher Intelligenz hat das Interesse der Menschheit seit vielen Jahrzehnten bewegt und wird seit den 1960er Jahren rege beforscht. Dieser Kurs gibt einen detaillierten Überblick über die historischen Entwicklungen, Erfolge und Rückschläge in der KI sowie die Entwicklung und den Einsatz von Expertensystemen in frühen KI-Systemen.Um kognitive Prozesse zu verstehen, wird der Kurs einen kurzen Überblick über das biologische Gehirn und (menschliche) kognitive Prozesse geben und sich dann auf die Entwicklung moderner KI-Systeme konzentrieren, die durch die jüngsten Entwicklungen im Bereich der Hard- und Software vorangetrieben werden. Besonderes Augenmerk liegt auf der Diskussion der Entwicklung "schmaler KI"-Systeme für spezifische Anwendungsfälle im Vergleich zur Schaffung allgemeiner künstlicher Intelligenz.Der Kurs gibt einen Überblick über ein breites Spektrum potenzieller Anwendungsbereiche der künstlichen Intelligenz, darunter Industriebereiche wie autonomes Fahren und Mobilität, Medizin, Finanzen, Einzelhandel und Produktion.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- sich einen Überblick über die historischen Entwicklungen im Bereich der künstlichen Intelligenz zu verschaffen.
- die verschiedenen Anwendungsbereiche der künstlichen Intelligenz zu analysieren.
- Expertensysteme zu verstehen.
- Prolog auf einfache Expertensysteme anzuwenden.
- das Gehirn und die kognitiven Prozesse aus neurowissenschaftlicher Sicht zu verstehen.
- moderne Entwicklungen in der künstlichen Intelligenz zu verstehen.

Kursinhalt

1. Geschichte der KI
   - 1.1 Historische Entwicklungen
   - 1.2 KI Winter
   - 1.3 Bemerkenswerte Fortschritte in der AI
2. Expertensysteme
   - 2.1 Überblick über Expertensysteme
   - 2.2 Einführung in Prolog

3. Neurowissenschaften
   - 3.1 Das (menschliche) Gehirn
   - 3.2 Kognitive Prozesse

4. Moderne KI-Systeme
   - 4.1 Jüngste Entwicklungen bei Hard- und Software
   - 4.2 Schmale vs. Allgemeine KI
   - 4.3 NLP und Computer Vision

5. AI Anwendungsbereiche
   - 5.1 Autonome Fahrzeuge & Mobilität
   - 5.2 Personalisierte Medizin
   - 5.3 FinTech
   - 5.4 Einzelhandel und Industrie

Literatur

Pflichtliteratur

Weiterführende Literatur

- Bear, F./Barry, W./Paradiso, M. (2006): Neuroscience: Exploring the brain. 3rd ed., Lippincott Williams and Wilkins, Baltimore, MD.
- Bratko, I. (2011): Prolog programming for artificial intelligence. 4th ed., Pearson, Hoboken, NJ.
- Jackson, P. (1998): Introduction to expert systems. 3rd ed., Addison Wesley Longman, Chicago, IL.
- Nilsson, N. (2009): The quest for artificial intelligence. Cambridge University Press, Cambridge.
- Russel, S./Norvig, P. (2009): Artificial intelligence: A modern approach. 3rd ed., Pearson, Malaysia.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Seminar: Künstliche Intelligenz und Gesellschaft

Kurscode: DLMAISAIS01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		5	keine

Beschreibung des Kurses

Im laufenden Jahrzehnt wurden auf dem Gebiet der künstlichen Intelligenz beeindruckende Fortschritte erzielt. Verschiedene kognitive Aufgaben wie die Objekterkennung in Bild und Video, die Verarbeitung natürlicher Sprache, die Spielstrategie und das autonome Fahren und die Robotik werden heute von Maschinen auf einem noch nie dagewesenen Niveau ausgeführt. In diesem Kurs werden einige der gesellschaftlichen, wirtschaftlichen und politischen Auswirkungen dieser Entwicklungen untersucht.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- ausgewählte aktuelle gesellschaftliche Themen und Fragestellungen der künstlichen Intelligenz zu nennen.
- den Einfluss und die Auswirkungen der künstlichen Intelligenz auf gesellschaftliche, wirtschaftliche und politische Themen zu erklären.
- theoretisch erworbenes Wissen auf reale Fälle zu übertragen.
- ein ausgewähltes Thema in Form eines schriftlichen Aufsatzes wissenschaftlich zu behandeln.
- aktuelle gesellschaftliche und politische Fragen, die sich aus den jüngsten Fortschritten in der Methodik der künstlichen Intelligenz ergeben, kritisch zu hinterfragen und zu diskutieren.
- eigene Problemlösungsfähigkeiten und -prozesse durch Reflexion über die möglichen Auswirkungen ihrer zukünftigen Tätigkeit im Bereich der künstlichen Intelligenz zu entwickeln.

Kursinhalt

- Das Seminar behandelt aktuelle Themen zu den gesellschaftlichen Auswirkungen der künstlichen Intelligenz. Alle Teilnehmenden erstellen eine Seminararbeit zu einem zugewiesenen Thema.

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Boddington, P. (2017): Towards a code of ethics for artificial intelligence. 1st ed., Springer International Publishing, New York, NY. ▪ Bostrom, N. (2016): Superintelligence: Paths, dangers, strategies. Oxford University Press, Oxford. ▪ Tegmark, M. (2018): Life 3.0: Being human in the age of artificial intelligence. Penguin, New York, NY. ▪ Wachter-Boettcher, S. (2017): Technically wrong: Sexist apps, biased algorithms, and other threats of toxic tech. W. W. Norton & Company, New York, NY.

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Seminar

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Seminararbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

DLMAISAIS01_D

Sichere Software-Entwicklung

Modulcode: DLMCSEEDSO_D

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	▪ keine ▪ DLMCSEEDSO01_D oder DLMCSEEDSO01_E	MA	10	300 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

N.N. Professorship Cyber Security (Sichere Software-Entwicklung) / N.N. Professorship Cyber Security (Projekt: Sichere Software-Implementierung)

Kurse im Modul

- Sichere Software-Entwicklung (DLMCSEEDSO01_D)
- Projekt: Sichere Software-Implementierung (DLMCSEEDSO02_D)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Sichere Software-Entwicklung • Studienformat "Fernstudium": Klausur, 90 Minuten Projekt: Sichere Software-Implementierung • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Projektbericht

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Sichere Software-Entwicklung

- Sicheres Software Design und -Implementierung
- Sicherheitsprüfung und -Auditierung
- Patch- und Schwachstellenmanagement
- Software-Lebenszyklus

Projekt: Sichere Software-Implementierung

- Sicheres Software Design und -Implementierung
- Sicherheitsprüfung und -Auditierung
- Patch- und Schwachstellenmanagement
- Software-Lebenszyklus

Qualifikationsziele des Moduls

Sichere Software-Entwicklung

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- sichere Anwendungen zu entwerfen.
- zu verstehen, was zu Software-Kompromittierung führt.
- gewöhnliche Kodierungsfehler zu vermeiden.
- den sicheren Software-Lebenszyklus zu steuern.
- ein strenges Sicherheitsprüfungssystem anzuwenden.
- die Offenlegung von Schwachstellen zu steuern.

Projekt: Sichere Software-Implementierung

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Sicherheitsmaßnahmen für ein einfaches Software-Projekt zu entwerfen.
- häufige Kodierungs- und Designfehler zu vermeiden.
- zu definieren, welche Schritte erforderlich sind, um sicheren Code zu implementieren.
- einen Prozess zu schaffen, der die kontinuierliche Sicherheit der Anwendung während ihrer gesamten Lebensdauer gewährleistet.
- die Offenlegung von Schwachstellen effektiv zu nutzen.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der IUBH**
Baut auf Modulen aus dem Bereich Informatik & Software-Entwicklung auf	Alle Master-Programme aus dem Bereich IT & Technik

Sichere Software-Entwicklung

Kurscode: DLMCSEEDSO01_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		5	keine

Beschreibung des Kurses

Der Angriff auf Schwachstellen in unsicherer Software ist ein führender Angriffsweg für Kriminelle und böswillige staatliche Akteure. Das Auffinden unbekannter so genannter Zero-Day-Schwachstellen ist ein zentrales Werkzeug für professionelle Kriminelle. Daher ist es von größter Bedeutung, sichere Software zu entwickeln und zu implementieren. Zuerst müssen wir allgemeine Softwareschwächen verstehen und diese dann so früh wie möglich in der Entwicklung und im Software-Lebenszyklus durch eine "Security-by-Design"-Philosophie vermeiden. Außerdem soll ein Prozess für Sicherheitstests und die Offenlegung von Schwachstellen durchgeführt und gesteuert werden. Die Entwicklung und Implementierung von zeitgerechten Softwareupdates „Patches“ ist essentiell.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- sichere Anwendungen zu entwerfen.
- zu verstehen, was zu Software-Kompromittierung führt.
- gewöhnliche Kodierungsfehler zu vermeiden.
- den sicheren Software-Lebenszyklus zu steuern.
- ein strenges Sicherheitsprüfungssystem anzuwenden.
- die Offenlegung von Schwachstellen zu steuern.

Kursinhalt

1. Security-by-Design
   - 1.1 IT-Unterstützung udn tests durch die “Shift Left” Methodologie
   - 1.2 Skriptbasierte Steuerung - Infrastruktur as a Code
   - 1.3 Vorteile einer frühzeitigen Berücksichtigung der Sicherheit
2. Privacy-by-Design
   - 2.1 Verschlüsselung
   - 2.2 Schutz der Privatsphäre durch Differentielm Privacy
   - 2.3 Zero-Knowledge-Beweise und Protokolle

3. Prüfung und Auditierung
   - 3.1 Prüfung der Unit
   - 3.2 Sicherheitsprüfung
   - 3.3 Prüfung von Sicherheitscodes

4. Sicherheit der Software-Lieferkette
   - 4.1 Sicherheit von Paketen
   - 4.2 Container-Sicherheit
   - 4.3 Überlegungen zur Programmiersprache

5. Gängige Programmierfehler
   - 5.1 Klassen von Fehlern
   - 5.2 Quellen von Fehlern
   - 5.3 Schweregrad der Fehler

6. Projektleitung
   - 6.1 Der Software-Lebenszyklus
   - 6.2 Umgang mit der Offenlegung von Schwachstellen
   - 6.3 Steuern von Patches/Aktualisierungen
   - 6.4 Steuern von Pentesting- und Bug-Bounty-Programmen

7. DevSecOps
   - 7.1 DevOps
   - 7.2 Cloud-Sicherheit
   - 7.3 Kontinuierliche Integration, Prüfung und Bereitstellung
   - 7.4 Kurzlebige Prozesse
   - 7.5 Automatisierung

Literatur

Pflichtliteratur

Weiterführende Literatur

- Adkins, H. et al (2020): Building Secure and Reliable Systems. 1st edition, O'Reilly Media, Newton, MA.
- Common Weakness Enumeration, https://cwe.mitre.org/
- Dwork, C. / Roth, A. (2014): The Algorithmic Foundations of Differential Privacy. In Foundations and Trends in Theoretical Computer Science Vol. 9, Nos. 3–4 (2014) 211–407.
- The Open Web Application Security Project, https://owasp.org/

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Online-Vorlesung

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Ja **Evaluation:** Nein
Prüfungsleistung	Klausur, 90 Minuten

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
90 h	0 h	30 h	30 h	0 h	150 h

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☑ Skript	☐ Creative Lab
☐ Vodcast	☐ Prüfungsleitfaden
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☑ Musterklausur	

Projekt: Sichere Software-Implementierung

Kurscode: DLMCSEEDSO02_D

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		5	DLMCSEEDSO01_D oder DLMCSEEDSO01_E

Beschreibung des Kurses

Frei nach dem Spruch „Software is eating the world“ kann es sich keine Organisation leisten, unsicheren Code einzusetzen, ohne letztendlich schlimme Folgen zu erleiden. In diesem Projekt sollen Studierende eine sichere Anwendungsimplementierung in Angriff nehmen und einen Bericht schreiben, in dem die getroffenen Entscheidungen zur Gewährleistung der Sicherheit des laufenden Systems begründet werden.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- Sicherheitsmaßnahmen für ein einfaches Software-Projekt zu entwerfen.
- häufige Kodierungs- und Designfehler zu vermeiden.
- zu definieren, welche Schritte erforderlich sind, um sicheren Code zu implementieren.
- einen Prozess zu schaffen, der die kontinuierliche Sicherheit der Anwendung während ihrer gesamten Lebensdauer gewährleistet.
- die Offenlegung von Schwachstellen effektiv zu nutzen.

Kursinhalt

- Für ein gegebenes Problem und/oder einen gegebenen Kontext entwirft und entwickelt der Studierende ein einfaches Softwareprojekt und reicht dann einen Bericht, Code und Daten ein, die die Entscheidungen des Sicherheitsdesigns sowie Pläne für den zukünftigen Software-Lebenszyklus beschreiben. Spezifische Projekte werden vom Tutor zur Verfügung gestellt, aber Vorschläge der Studierenden können berücksichtigt werden.

Literatur

Pflichtliteratur

Weiterführende Literatur

- Adkins, H. et al (2020): Building Secure and Reliable Systems. 1st edition, O’Reilly Media, Newton, MA.
- Common Weakness Enumeration, https://cwe.mitre.org/
- Dwork, C. / Roth, A. (2014): The Algorithmic Foundations of Differential Privacy. In Foundations and Trends in Theoretical Computer Science Vol. 9, Nos. 3–4 (2014) 211–407.
- The Open Web Application Security Project, https://owasp.org/

Studienformat Fernstudium

Studienform	**Kursart**
Fernstudium	Projekt

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Projektbericht

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
120 h	0 h	30 h	0 h	0 h	150 h

Lehrmethoden	
☐ Learning Sprints®	☐ Repetitorium
☐ Skript	☐ Creative Lab
☐ Vodcast	☑ Prüfungsleitfaden
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Musterklausur	

DLMCSEEDSO02_D

Blockchain and Quantum Computing

Module Code: DLMCSEBCQC

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	None	MA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Rald Kneuper (Blockchain) / Dr. Carsten Blank (Quantum Computing)

Contributing Courses to Module

- Blockchain (DLMCSEBCQC01)
- Quantum Computing (DLMCSEBCQC02)

Module Exam Type

Module Exam	Split Exam
	Blockchain • Study Format "Distance Learning": Written Assessment: Written Assignment Quantum Computing • Study Format "Distance Learning": Oral Assignment

Weight of Module

see curriculum

Module Contents

Blockchain

- Basic concepts of blockchain and related technologies
- Applications of blockchain and DLT
- Security
- Development of blockchain and DLT applications
- Social and legal aspects

Quantum Computing

- Physics of quantum computing
- Quantum computing models
- Quantum algorithms
- Quantum computing with the IBM framework Qiskit
- Applications, potential for and challenges of quantum computing

Learning Outcomes

Blockchain

On successful completion, students will be able to

- outline the functions provided by and the technology used in blockchains.
- explain important applications of block chains, in particular BitCoin.
- demonstrate the technical architecture of blockchain applications.
- appraise the benefits and challenges of suggested blockchain applications.
- discuss the social and legal aspects of blockchain technology.

Quantum Computing

On successful completion, students will be able to

- outline the basic concepts of quantum mechanics as they relate to quantum computing.
- describe the computation models used in quantum computing.
- demonstrate the role of quantum computing for cryptography and other application areas.
- compare the theoretical and practical potential of quantum computing to classical computing.
- apply the concepts of quantum computing to develop simple programs within the Qiskit framework.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the field of Computer Science & Software Development.	All Bachelor Programmes in the IT & Technology field.

Blockchain

Course Code: DLMCSEBCQC01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
MA	English		5	None

Course Description

Started by the cryptocurrency BitCoin, blockchain and related topics such as distributed ledger technologies and smart contracts have become increasingly important over the last few years and are claimed to be a major disruptive technologies. As BitCoin shows, systems that today need a trustworthy central coordinating body may become genuinely distributed systems without the need for such a body in the future. While blockchain has the potential for completely new types of applications, these suggested applications do not always make use of the strengths of the technology; rather, they simply provide a different approach to solving problems that could be solved more easily and efficiently using standard technologies such as database systems. Furthermore, blockchain applications have led to new social challenges and legal questions, such as the legal status of “smart contracts”. Different infrastructures such as Ethereum and Hyperledger have been developed to form the basis for blockchain applications. The goal of this course is to provide an understanding of the technical, as well as social and legal, aspects of blockchain and related technologies.

Course Outcomes

On successful completion, students will be able to

- outline the functions provided by and the technology used in blockchains.
- explain important applications of block chains, in particular BitCoin.
- demonstrate the technical architecture of blockchain applications.
- appraise the benefits and challenges of suggested blockchain applications.
- discuss the social and legal aspects of blockchain technology.

Contents

1. Basic Concepts
   - 1.1 The Functional View: Distributed Ledger Technologies
   - 1.2 The Technical View: Blockchain
   - 1.3 History of Blockchain and DLT
   - 1.4 Consense Mechanisms

2. BitCoin
   - 2.1 The BitCoin Payment System
   - 2.2 The Technology Behind BitCoin
   - 2.3 Security of BitCoin
   - 2.4 Scalability and Other Limitations of BitCoin
   - 2.5 BitCoin Derivatives and Alternatives

3. Smart Contracts and Decentralized Apps
   - 3.1 Smart Contracts
   - 3.2 Decentralized Apps (DApps)
   - 3.3 Ethereum
   - 3.4 Hyperledger
   - 3.5 Alternative Platforms for Smart Contracts and DApps

4. Security of Block Chain and DLT
   - 4.1 Cryptology Used
   - 4.2 Attacks on Blockchain and DLT
   - 4.3 Resolving Bugs and Security Holes
   - 4.4 Long-Term Security

5. Block Chain and DLT Application Scenarios
   - 5.1 Benefits and Limits of Applying Blockchain and DLT
   - 5.2 Registers for Land and Other Property
   - 5.3 Applications in the Supply Chain
   - 5.4 Applications in Insurance
   - 5.5 Initial Coin Offerings for Sourcing Capital
   - 5.6 Examples of Further Applications

6. Development of Blockchain and DLT Applications
   - 6.1 Architecture of Blockchain and DLT Applications
   - 6.2 Platform Selection
   - 6.3 Design of Blockchain and DLT Applications

7. Blockchain and Society
   - 7.1 (Mis-)Trust in Institutions
   - 7.2 Blockchain and the Environment
   - 7.3 Cyber-Currencies in the Darknet
   - 7.4 ICO Fraud

8. Legal Aspects
   - 8.1 DLT and Smart Contracts as Legal Contracts
   - 8.2 Cryptocurrencies as Legal Currencies
   - 8.3 Regulation of ICOs
   - 8.4 Data Protection / Privacy in Blockchains

Literature

Compulsory Reading

Further Reading

- De Filippi, P., & Wright, A. (2018). Blockchain and the law. The rule of code. Cambridge, MA: Harvard University Press.
- Meinel, C., Gayvoronskaya, T. & Schnjakin, M. (2018). Blockchain. Hype or innovation. Potsdam: Universitätsverlag Potsdam.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system [white paper]. Retrieved from https://bitcoin.org/bitcoin.pdf
- Tapscott, D., & Tapscott, N. (2018). Blockchain revolution. How the technology behind bitcoin is changing money, business, and the world. New York, NY: Portfolio/Penguin.
- Xu, W., Weber, I., & Staples, M. (2019). Architecture for blockchain applications. Cham: Springer.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Written Assessment: Written Assignment

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☑ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

Quantum Computing

Course Code: DLMCSEBCQC02

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Quantum computing is a completely new paradigm for the architecture of computers. It currently is in the early stage of development but has the potential to speed up certain kinds of computations, not just by orders of magnitude but by moving them from exponential to linear growth. One of the issues that will be affected is the prime factorization of large numbers which currently forms the basis for important cryptographic algorithms, in particular the RSA algorithm which would in that case would no longer be secure. This course gives an introduction to the physics behind quantum computing and the computation models used. Students are familiarized with the most important algorithms for quantum computing and write a few programs for quantum computers. The application potential and challenges of quantum computing are also discussed.

Course Outcomes

On successful completion, students will be able to

- outline the basic concepts of quantum mechanics as they relate to quantum computing.
- describe the computation models used in quantum computing.
- demonstrate the role of quantum computing for cryptography and other application areas.
- compare the theoretical and practical potential of quantum computing to classical computing.
- apply the concepts of quantum computing to develop simple programs within the Qiskit framework.

Contents

1. Basic concepts
   - 1.1 Quantum physics as a basis for computing
   - 1.2 Types of quantum computers
   - 1.3 Qbits
   - 1.4 Linear algebra

2. The physics of quantum computers
   - 2.1 Basic concepts of quantum mechanics
   - 2.2 Spin and entanglement
   - 2.3 Architecture of quantum computers
   - 2.4 Noise and error correction
   - 2.5 Current state and outlook

3. Quantum computing models
   - 3.1 Quantum gates and circuits
   - 3.2 Single qubit quantum systems
   - 3.3 Multiple qubit quantum systems

4. Quantum algorithms
   - 4.1 Computability and complexity in quantum computing
   - 4.2 Quantum Fourier transform
   - 4.3 The Shor algorithm
   - 4.4 The Grover algorithm

5. Quantum computing with the IBM framework Qiskit
   - 5.1 Overview of Qiskit and the IBM Q Provider
   - 5.2 Quantum circuits in Qiskit
   - 5.3 First steps in programming with Qiskit

6. Applications, potential and challenges of quantum computing
   - 6.1 Applications of quantum computing
   - 6.2 Quantum cryptography and post-quantum cryptography
   - 6.3 Quantum supremacy

Literature
Compulsory Reading
Further Reading ▪ Bernhardt, C. (2019): Quantum computing for everyone. MIT Press, Cambridge, MA. ▪ Faro, I. (2017): A developer's guide to using the Quantum QISKit SDK. Retrieved from https://developer.ibm.com/code/2017/05/17/developers-guide-to-quantum-qiskit-sdk/ ▪ Rieffel, E. G. (2014): Quantum computing. A gentle introduction. MIT Press, Cambridge, MA. ▪ Susskind, L. / Friedman, A. (2015): Quantum mechanics. The theoretical minimum. Penguin, London. ▪ Zygelman, B. (2018): A first introduction to quantum computing and information. Springer, Cham.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Oral Assignment

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☐ Exam Template	

Continuous and Lifecycle Security

Module Code: DLMCSEECLS_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	none	MA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Alexander Lawall (Cyber Resilience) / Prof. Dr. Jesus Luna Garcia (Seminar: Applying Threat Intelligence)

Contributing Courses to Module

- Cyber Resilience (DLMCSEECLS01_E)
- Seminar: Applying Threat Intelligence (DLMCSEECLS02_E)

Module Exam Type

Module Exam	Split Exam
	Cyber Resilience • Study Format "Distance Learning": Exam, 90 Minutes Seminar: Applying Threat Intelligence • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module

see curriculum

Module Contents

Cyber Resilience

- Cyber resilience
- DevSecOps
- Threat Intelligence
- Crisis Management
- Security Culture

Seminar: Applying Threat Intelligence

- Cyber resilience
- DevSecOps
- Threat Intelligence
- Crisis Management
- Security Culture

Learning Outcomes

Cyber Resilience

On successful completion, students will be able to

- implement defense in depth and fault tolerance.
- work with resilience frameworks.
- use threat intelligence to design better resilience.
- use DevSecOps practices to improve resilience.
- manage crises that arise from attacks and corporate culture.

Seminar: Applying Threat Intelligence

On successful completion, students will be able to

- understand weaknesses in an organization's defenses.
- make recommendations on how to make the organization more resilient.
- utilize threat intelligence for secure application and systems design.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Master Programs in the IT & Technology fields

Cyber Resilience

Course Code: DLMCSEECLS01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Even with state-of-the-art security controls in place, attacks will still be successful with enough persistence, and state actors and some criminals have shown a willingness to go that extra mile to penetrate their target. A resilient organization will have the monitoring and procedures in place and rapidly detect, triage and react to any attack. Furthermore, this organization will have enough fault tolerance so that an attack cannot affect the entire organization at the same time.

Course Outcomes

On successful completion, students will be able to

- implement defense in depth and fault tolerance.
- work with resilience frameworks.
- use threat intelligence to design better resilience.
- use DevSecOps practices to improve resilience.
- manage crises that arise from attacks and corporate culture.

Contents

1. Defense in depth
   - 1.1 The fallacy of complete security
   - 1.2 Byzantine fault tolerance
   - 1.3 Intrusion and fault detection
   - 1.4 Layers of protection
2. Design Principles
   - 2.1 Least Privilege
   - 2.2 Role and domain separation
   - 2.3 Revocation and Rollback
   - 2.4 Towards an anti-fragile organization
3. Fault tolerance
   - 3.1 Data protection and lifecycle
   - 3.2 Distributed and redundant data processing
   - 3.3 Applications of Blockchain technology

4. Frameworks
   - 4.1 NIST Cyber resilience engineering framework
   - 4.2 OODA-loop: Observe. Orient. Decide. Act.

5. Threat Intelligence
   - 5.1 Techniques, Tactics and Procedures
   - 5.2 Common weaknesses
   - 5.3 Threat Intelligence data

6. DevSecOps best practices
   - 6.1 Ephemeral processes
   - 6.2 Tiered data storage
   - 6.3 Continuous integration, testing and deployment with Caneries
   - 6.4 Availability zones for data and processes
   - 6.5 Avoiding complexity

7. Crisis management
   - 7.1 The Incident Response team
   - 7.2 Incident triage
   - 7.3 Communication
   - 7.4 Recovery planning and execution
   - 7.5 Postmortem

8. Organization and Culture
   - 8.1 Roles and responsibilities
   - 8.2 Security as a first-class citizen in an organization
   - 8.3 Influencing corporate culture
   - 8.4 Leadership buy-in

Literature
Compulsory Reading
Further Reading ▪ Adkins, H. et al (2020): Building Secure and Reliable Systems. First Edition, O'Reilly Media, Newton, MA. ▪ Ross, R. et al (2019): Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 800-160 Volume 2. https://doi.org/10.6028/NIST.SP.800-160v2 ▪ Ross, R. / McEvilley, M. / Oren, J. C. (2016): Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Includes updates as of March 21, 2018. https://doi.org/10.6028/NIST.SP.800-160v1

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Seminar: Applying Threat Intelligence

Course Code: DLMCSEECLS02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

Cyber resilience is the practice of accepting that security will never be 100% watertight but the ability to limit damage and quickly detect and respond to incidents is of utmost importance. In this seminar, we examine reports from past incidents and identify threat intelligence, in particular the Techniques, Tactics and Procedures of criminals, that help in identifying effective defenses.

Course Outcomes

On successful completion, students will be able to

- understand weaknesses in an organization's defenses.
- make recommendations on how to make the organization more resilient.
- utilize threat intelligence for secure application and systems design.

Contents

- With a given report, the student will research the incident and independently find threat intelligence reports and data relevant to the given incident. A report will then summarize the security issues responsible for the incident and make recommendations as to how the victim could become more resilient to such attacks. Specific incident reports will be provided by the tutor but proposals by the students can be considered.

Literature

Compulsory Reading

Further Reading

- Adkins, H. et al (2020): Building Secure and Reliable Systems. First Edition, O'Reilly Media, Inc.
- Mitre ATT&CK®: https://attack.mitre.org/
- OASIS Cyber Threat Intelligence: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti
- Ross, R. et al (2019): Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 800-160 Volume 2. https://doi.org/10.6028/NIST.SP.800-160v2

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Audit- and Security Testing

Module Code: DLMCSEEAST_E

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ none ▪ DLMCSEEAST01_E	MA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Alexander Lawall (Attack Models and Auditing) / Prof. Dr. Jesus Luna Garcia (Seminar: IT Security Tests)

Contributing Courses to Module

- Attack Models and Auditing (DLMCSEEAST01_E)
- Seminar: IT Security Tests (DLMCSEEAST02_E)

Module Exam Type

Module Exam	Split Exam
	Attack Models and Auditing • Study Format "Distance Learning": Exam, 90 Minutes Seminar: IT Security Tests • Study Format "Distance Learning": Written Assessment: Research Essay

Weight of Module

see curriculum

Module Contents

Attack Models and Auditing

- Threat modelling
- Software testing and verification
- Pentesting tools
- Self-assessment and third-party audits
- Ethical hacking

Seminar: IT Security Tests

Software and system auditing; Pentesting; Red/Blue teams; Bug Bounty programs

Learning Outcomes

Attack Models and Auditing

On successful completion, students will be able to

- plan what to test and audit for.
- understand common pentesting tools.
- understand software testing and verification.
- organize self-assessments of the implemented ISMS.
- familiarize with widely used cybersecurity audit frameworks.
- run remote system audits.

Seminar: IT Security Tests

On successful completion, students will be able to

- understand how bug bounty programs work.
- understand how to run a red/blue team or pentesting exercise.
- write a report showing aptitude in the subject.

Links to other Modules within the Study Program	Links to other Study Programs of IUBH
This module is similar to other modules in the fields of Computer Science & Software Development	All Master Programs in the IT & Technology fields

Attack Models and Auditing

Course Code: DLMCSEEAST01_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
MA	English		5	none

Course Description

The cybersecurity lifecycle comprehends a range of activities, where “checking” the implemented security concept provides a feedback loop to continuously improve the designed security levels. In practice, cybersecurity checks include an initial threat modeling step before the right tools and techniques can be used to test the security of the software or system. This can be a type of ethical hacking (e.g., pentesting, red/blue team exercise or bug bounty program), or a self-assessment or this-party audit of the deployed information security management system (ISMS).

Course Outcomes

On successful completion, students will be able to

- plan what to test and audit for.
- understand common pentesting tools.
- understand software testing and verification.
- organize self-assessments of the implemented ISMS.
- familiarize with widely used cybersecurity audit frameworks.
- run remote system audits.

Contents

1. Threat Modelling
   - 1.1 System Security Life Cycle
   - 1.2 Modelling applications and profiling threats
   - 1.3 Security testing based on a threat model
   - 1.4 OWASP Threat Dragon and Microsoft Threat Modelling Tool
2. Ethical Hacking
   - 2.1 Legal and compliance framework
   - 2.2 Pentesting process
   - 2.3 Red/Blue teams
   - 2.4 Bug bounty programs

3. Multi-layer system security testing
   - 3.1 Operating system exploits
   - 3.2 Network penetration testing and tools
   - 3.3 Web app penetration testing with OWASP and OSINT
   - 3.4 Exploit development

4. Software testing
   - 4.1 Whitebox, blackbox and graybox testing
   - 4.2 Unit testing for security
   - 4.3 Fuzzing
   - 4.4 ISO/IEC 29119

5. Software verification
   - 5.1 Static code analysis
   - 5.2 Dynamic code analysis
   - 5.3 Peer review
   - 5.4 Formal verification

6. Cybersecurity Audits
   - 6.1 Self-assessments and third-party audits
   - 6.2 Risk-based approach to cybersecurity checks
   - 6.3 Auditing cybersecurity based on ISO/IEC 27001
   - 6.4 Toolset for automated audits

Literature

Compulsory Reading

Further Reading

- Bellovin, S. M. (2016): Thinking Security. Stopping Next Year's Hackers. Addison-Wesley, Boston, MA.
- Joint Task Force Transformation Initiative (2012): Guide for Conducting Risk Assessments. Revision 1, NIST Computer Security Division. (URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final [Retrieved: 11.03.2021]).
- Kim, P. (2014): The Hacker Playbook. A Practical Guide to Penetration Testing. CreateSpace Independent Publishing Platform. 4th Edition. (URL: https://www.isaca.org/bookstore/audit-control-and-security-essentials/witaf4 [Retrieved: 11.03.2021]).
- Information Systems Audit and Control Association (2020): IT Audit Framework (ITAF). A Professional Practices Framework for IT Audit. Isaca, Rolling Meadows, IL.
- Schneier, B. (1999): Attack Trees. (URL: https://www.schneier.com/academic/archives/1999/12/attack_trees.html [Retrieved: 11.3.2021]).
- Shostack, A. (2014): Threat Modeling. Designing for Security. John Wiley & Sons, Hoboken, NJ.

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** no
Type of Exam	Exam, 90 Minutes

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
90 h	0 h	30 h	30 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☑ Course Book	☐ Creative Lab
☐ Vodcast	☐ Guideline
☑ Shortcast	☐ Live Tutorium/Course Feed
☑ Audio	
☑ Exam Template	

Seminar: IT Security Tests

Course Code: DLMCSEEAST02_E

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
MA	English		5	DLMCSEEAST01_E

Course Description

A good security architecture is a fine thing, but it is always better to test it than to find out too late that there was one more hole to patch. In this seminar, the student will complete a report on a security audit method. This can be a type of pentesting, red/blue team exercise or bug bounty program. Alternatively, the report can cover a vulnerability report created from a public bug bounty program. The intension is that the student has the opportunity to go in depth with an aspect of this subject.

Course Outcomes

On successful completion, students will be able to

- understand how bug bounty programs work.
- understand how to run a red/blue team or pentesting exercise.
- write a report showing aptitude in the subject.

Contents

- Testing security is just as important as implementing it. This seminar will address this topic with reports on a variety of subjects the student can choose from. The student will use current literature to research the topic and write a report on it. Possible topics can be based on tools in the areas of WWW pentesting, fuzzing, code security auditing. Or topics can be chosen from playbooks from red and blue teams. Or the student may choose to look into best practices for setting up and managing bug bounty programs.

Literature
Compulsory Reading
Further Reading ▪ Kim, P. (2014): The Hacker Playbook: Practical Guide To Penetration Testing. CreateSpace Independent Publishing Platform, Scotts Valley, CA. ▪ Kim, P. (2015): The Hacker Playbook 2: Practical Guide To Penetration Testing. CreateSpace Independent Publishing Platform, Scotts Valley, CA. ▪ Kim, P. (2018): The Hacker Playbook 3: Practical Guide To Penetration Testing. CreateSpace Independent Publishing Platform, Scotts Valley, CA. ▪ Klein, T. (2011): A Bug Hunter's Diary: A Guided Tour Through the Wilds of Software Security. No Starch Press, San Francisco, CA. ▪ McClure, S. / Scambray, J. / Kurtz, G. (2012): Hacking Exposed 7, McGraw-Hill, New York City, NY. ▪ The Zero-day Initiative blog: https://www.zerodayinitiative.com/blog

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☐ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

DLMCSEEAST02_E

Advanced Cyber Security and Cryptology

Module Code: DLMCSEAITSC

Module Type	Admission Requirements	Study Level	CP	Student Workload
see curriculum	▪ DLMCSITSDP01 or DLMCSITSDS01 ▪ DLMCSEAITSC01; DLMCSITSDP01 or DLMCSITSDS01	MA	10	300 h

Semester / Term	Duration	Regularly offered in	Language of Instruction
see curriculum	Minimum 1 semester	WiSe/SoSe	English

Module Coordinator

Prof. Dr. Alexander Lawall (Seminar: Advanced Cyber Security) / Prof. Dr. Ralf Kneuper (Cryptology)

Contributing Courses to Module

- Seminar: Advanced Cyber Security (DLMCSEAITSC01)
- Cryptology (DLMCSEAITSC02)

Module Exam Type

Module Exam	Split Exam
	Seminar: Advanced Cyber Security • Study Format "Distance Learning": Written Assessment: Research Essay Cryptology • Study Format "Distance Learning": Oral Assignment

Weight of Module

see curriculum

Module Contents

Seminar: Advanced Cyber Security

- This course covers selected advanced topics in cyber security, including the closely related topics of data protection and cryptology, and discusses them in detail. Based on a list of topics updated regularly, students select or are assigned a specific topic about which they write a scientific research essay.

Cryptology

- Symmetric and asymmetric cryptosystems
- Authentication
- Cryptanalysis
- Cryptology in the internet
- Applications

Learning Outcomes

Seminar: Advanced Cyber Security

On successful completion, students will be able to

- analyze and describe one aspect of cyber security in detail.
- independently analyze selected topics in cyber security and link them with well-known concepts, as well as critically question and discuss them.
- transfer theoretically-acquired knowledge to a specific context.
- write and edit a scientific essay on a relevant select topic.

Cryptology

On successful completion, students will be able to

- discuss the main cryptographic systems and algorithms and their relevance in IT today.
- discuss the security of internet-based applications.
- evaluate different cryptographic systems and algorithms to select an appropriate solution for real-world problems in IT.
- apply standard cryptographic systems and algorithms to solve real-world problems in IT.
- appraise existing cryptographic solutions to real-world problems and identify major weaknesses where relevant.

Links to other Modules within the Study Program	**Links to other Study Programs of IUBH**
This module is similar to other modules in the field of Computer Science & Software Development	All Master Programmes in the IT & Technology field

Seminar: Advanced Cyber Security

Course Code: DLMCSEAITSC01

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
MA	English		5	DLMCSITSDP01 or DLMCSITSDS01

Course Description

This seminar covers advanced topics in cyber security. With the growth of the internet and digitization, cyber security has become an increasingly important topic and needs to be taken into account in the development and setup of software and IT systems. Typical topics that may be addressed include the analysis of selected aspects of information security management systems according to the ISO 27000 series; the use of cyber security to support data protection; and the detailed analysis and description of certain algorithms or cryptosystems.

Course Outcomes

On successful completion, students will be able to

- analyze and describe one aspect of cyber security in detail.
- independently analyze selected topics in cyber security and link them with well-known concepts, as well as critically question and discuss them.
- transfer theoretically-acquired knowledge to a specific context.
- write and edit a scientific essay on a relevant select topic.

Contents

- The seminar covers different advanced topics regarding cyber security. Each participant must prepare a research essay on a topic assigned to him/her.

Literature
Compulsory Reading
Further Reading ▪ Bowman, C. et al. (2015). The architecture of privacy. On engineering technologies that can deliver trustworthy safeguards. O'Reilly, Sebastopol, CA:. ▪ Hintzbergen, J. et al. (2015): Foundations of information security. 3rd ed., Van Haren Publishing, Zaltbommel. ▪ ISO/IEC 29100 (2011): Information technology — Security techniques — Privacy framework. ISO. (URL: https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip [Retrieved: 22.3.2020]). ▪ Paar, C./Pelzl, J. (2011). Understanding cryptography: A textbook for students and practitioners. Springer, Heidelberg. ▪ The Open Web Application Security Project (OWASP) (2005): A guide to building secure web applications and web services. OWASP. (URL: https://www.um.es/atica/documentos/OWASPGuide2.0.1.pdf [Retrieved: 22.3.2020]).

Study Format Distance Learning

Study Format	Course Type
Distance Learning	Seminar

Information about the examination	
Examination Admission Requirements	**BOLK:** no **Course Evaluation:** no
Type of Exam	Written Assessment: Research Essay

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
120 h	0 h	30 h	0 h	0 h	150 h

Instructional Methods	
☐ Learning Sprints®	☐ Review Book
☐ Course Book	☐ Creative Lab
☐ Vodcast	☑ Guideline
☐ Shortcast	☑ Live Tutorium/Course Feed
☐ Audio	
☐ Exam Template	

Cryptology

Course Code: DLMCSEAITSC02

Study Level	Language of Instruction	Contact Hours	CP	Admission Requirements
MA	English		5	DLMCSEAITSC01; DLMCSITSDP01 or DLMCSITSDS01

Course Description

The focus of this course is to provide a thorough introduction to cryptology and its main sub-disciplines cryptography and cryptanalysis. Particular emphasis is put on the use of cryptology to support the security of IT systems. In the first part of the courses, students gain a solid understanding of the basic concepts of cryptology, in particular symmetric and asymmetric cryptosystems, authentication, and common approaches to break these cryptosystems using cryptanalysis. Based on this foundational understanding, the course goes on to cover the practical use of cryptology, starting with an introduction to the standard protocols and techniques used to ensure the security of communication via the internet. Next, practical aspects of applying cryptographic techniques and algorithms are covered, such as their long-term security. Finally, some application examples show how the concepts of cryptology are commonly used and can be used to solve challenges such as online banking.

Course Outcomes

On successful completion, students will be able to

- discuss the main cryptographic systems and algorithms and their relevance in IT today.
- discuss the security of internet-based applications.
- evaluate different cryptographic systems and algorithms to select an appropriate solution for real-world problems in IT.
- apply standard cryptographic systems and algorithms to solve real-world problems in IT.
- appraise existing cryptographic solutions to real-world problems and identify major weaknesses where relevant.

Contents

1. Basic concepts of cryptology
   - 1.1 Introduction and terminology
   - 1.2 IT security, threats and common attacks
   - 1.3 Historical overview
   - 1.4 Kerckhoffs's principle

2. Symmetric cryptosystems
   - 2.1 Substitution and transposition
   - 2.2 Stream and block ciphers
   - 2.3 Digital encryption standard (DES)
   - 2.4 Advanced encryption standard (AES)

3. Asymmetric cryptosystems
   - 3.1 The RSA algorithm
   - 3.2 Elliptic curves
   - 3.3 Cryptographic hash functions
   - 3.4 Signatures and MACs
   - 3.5 Key exchange and public key infrastructures

4. Authentication
   - 4.1 Passwords
   - 4.2 Challenge-response and zero-knowledge
   - 4.3 Biometrics-based authentication
   - 4.4 Authentication in distributed systems
   - 4.5 Smartcards
   - 4.6 Identity and anonymity

5. Cryptanalysis – how to break encryption
   - 5.1 Frequency analysis
   - 5.2 Brute-force attacks
   - 5.3 Rainbow tables
   - 5.4 Known/chosen plaintext
   - 5.5 Side-channel attacks

6. Cryptology and the internet
   - 6.1 Basic setup of the Internet and its protocols
   - 6.2 IPSec
   - 6.3 Transport Layer Security
   - 6.4 Secure E-Mail (TLS, S/MIME and PGP)
   - 6.5 Secure DNS

7. Practical aspects of cryptology
   - 7.1 Random number generation
   - 7.2 Long-term security (key lengths, perfect forward security, quantum computing)
   - 7.3 Incorporating cryptography into application development
   - 7.4 Legal and regulatory aspects

8. Applications
   - 8.1 Online banking
   - 8.2 Blockchain
   - 8.3 Voting
   - 8.4 Steganography and watermarks
   - 8.5 The Tor Project

Literature

Compulsory Reading

Further Reading

- Beutelspacher, A. (1994). Cryptology. Washington, DC: Mathematical Association of America.
- Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography engineering. Design principles and practical applications. Indianapolis, IN: Wiley.
- Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of applied cryptography. Boca Raton, FL: CRC Press.
- Paar, C., & Pelzl, J. (2011). Understanding cryptography: A textbook for students and practitioners. Berlin, Heidelberg: Springer.
- Singh, S. (2002). The code book: The secret history of codes and code-breaking. New York, NY: Harper Collins.

Study Format Distance Learning

Study Format	**Course Type**
Distance Learning	Online Lecture

Information about the examination	
Examination Admission Requirements	**BOLK:** yes **Course Evaluation:** yes
Type of Exam	Oral Assignment

Student Workload					
Self Study	**Presence**	**Tutorial**	**Self Test**	**Practical Experience**	**Hours Total**
110 h	0 h	20 h	20 h	0 h	150 h

Instructional Methods

- ☐ Learning Sprints®
- ☑ Course Book
- ☐ Vodcast
- ☑ Shortcast
- ☑ Audio
- ☐ Exam Template
- ☐ Review Book
- ☐ Creative Lab
- ☑ Guideline
- ☑ Live Tutorium/Course Feed

Masterarbeit

Modulcode: DLMMAB

Modultyp	Zugangsvoraussetzungen	Niveau	ECTS	Zeitaufwand Studierende
s. Curriculum	Gemäß Studien- und Prüfungsordnung	MA	15	450 h

Semester	Dauer	Regulär angeboten im	Unterrichtssprache
s. Curriculum	Minimaldauer: 1 Semester	WiSe/SoSe	Deutsch

Modulverantwortliche(r)

Studiengangsleiter (SGL) (Masterarbeit) / Studiengangsleiter (SGL) (Kolloquium)

Kurse im Modul

- Masterarbeit (DLMMAB01)
- Kolloquium (DLMMAB02)

Art der Prüfung(en)

Modulprüfung	Teilmodulprüfung
	Masterarbeit • Studienformat "Fernstudium": Schriftliche Ausarbeitung: Masterarbeit (90) Kolloquium • Studienformat "Fernstudium": Kolloquium (10)

Anteil der Modulnote an der Gesamtnote

s. Curriculum

Lehrinhalt des Moduls

Masterarbeit

- Masterarbeit

Kolloquium

- Kolloquium zur Masterarbeit

Qualifikationsziele des Moduls

Masterarbeit

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- eine Problemstellung aus ihrem Studienschwerpunkt unter Anwendung der fachlichen und methodischen Kompetenzen, die sie im Studium erworben haben, zu bearbeiten.
- eigenständig – unter fachlich-methodischer Anleitung eines akademischen Betreuers – ausgewählte Aufgabenstellungen mit wissenschaftlichen Methoden zu analysieren, kritisch zu bewerten sowie entsprechende Lösungsvorschläge zu erarbeiten.
- eine dem Thema der Masterarbeit angemessene Erfassung und Analyse vorhandener (Forschungs-)Literatur vorzunehmen.
- eine ausführliche schriftliche Ausarbeitung unter Einhaltung wissenschaftlicher Methoden zu erstellen.

Kolloquium

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- eine Problemstellung aus ihrem Studienschwerpunkt unter Beachtung akademischer Präsentations- und Kommunikationstechniken vorzustellen.
- das in der Masterarbeit gewählte wissenschaftliche und methodisch Vorgehen reflektiert darzustellen.
- themenbezogene Fragen von Fachexperten (Gutachter der Masterarbeit) aktiv zu beantworten.

Bezüge zu anderen Modulen im Studiengang	**Bezüge zu anderen Studiengängen der IUBH**
Alle Module im Masterprogramm	Alle Masterprogramme im Fernstudium

Masterarbeit

Kurscode: DLMMAB01

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		13.5	Gemäß Studien- und Prüfungsordnung

Beschreibung des Kurses

Ziel und Zweck der Masterarbeit ist es, die im Verlauf des Studiums erworbenen fachlichen und methodischen Kompetenzen in Form einer akademischen Abschlussarbeit mit thematischem Bezug zum Studienschwerpunkt erfolgreich anzuwenden. Inhalt der Masterarbeit kann eine praktisch-empirische oder aber theoretisch-wissenschaftliche Problemstellung sein. Studierende sollen unter Beweis stellen, dass sie eigenständig unter fachlich-methodischer Anleitung eines akademischen Betreuers eine ausgewählte Problemstellung mit wissenschaftlichen Methoden analysieren, kritisch bewerten und Lösungsvorschläge erarbeiten können. Das von dem Studierenden zu wählende Thema aus dem jeweiligen Studienschwerpunkt soll nicht nur die erworbenen wissenschaftlichen Kompetenzen unter Beweis stellen, sondern auch das akademische Wissen des Studierenden vertiefen und abrunden, um seine Berufsfähigkeiten und -fertigkeiten optimal auf die Bedürfnissen des zukünftigen Tätigkeitsfeldes auszurichten.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- eine Problemstellung aus ihrem Studienschwerpunkt unter Anwendung der fachlichen und methodischen Kompetenzen, die sie im Studium erworben haben, zu bearbeiten.
- eigenständig – unter fachlich-methodischer Anleitung eines akademischen Betreuers – ausgewählte Aufgabenstellungen mit wissenschaftlichen Methoden zu analysieren, kritisch zu bewerten sowie entsprechende Lösungsvorschläge zu erarbeiten.
- eine dem Thema der Masterarbeit angemessene Erfassung und Analyse vorhandener (Forschungs-)Literatur vorzunehmen.
- eine ausführliche schriftliche Ausarbeitung unter Einhaltung wissenschaftlicher Methoden zu erstellen.

Kursinhalt

- Im Rahmen der Masterarbeit muss die Problemstellung sowie das wissenschaftliche Untersuchungsziel klar herausgestellt werden. Die Arbeit muss über eine angemessene Literaturanalyse den aktuellen Wissensstand des zu untersuchenden Themas widerspiegeln. Der Studierende muss seine Fähigkeit unter Beweis stellen, das erarbeitete Wissen in Form einer eigenständigen und problemlösungsorientierten Anwendung theoretisch und/oder empirisch zu verwerten.

Literatur
Pflichtliteratur
Weiterführende Literatur ▪ Hunziker, A.W. (2010): Spass am wissenschaftlichen Arbeiten. So schreiben Sie eine gute Semester-, Bachelor- oder Masterarbeit. 4. Auflage, SKV, Zürich. ▪ Wehrlin, U. (2010): Wissenschaftliches Arbeiten und Schreiben. Leitfaden zur Erstellung von Bachelorarbeit, Masterarbeit und Dissertation – von der Recherche bis zur Buchveröffentlichung. AVM, München.

Studienformat Fernstudium

Studienform	Kursart
Fernstudium	Thesis-Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Schriftliche Ausarbeitung: Masterarbeit

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
405 h	0 h	0 h	0 h	0 h	405 h

Lehrmethoden
Die Studierenden schreiben ihre Masterarbeit eigenständig unter der methodischen und wissenschaftlicher Anleitung eine akademischen Betreuers.

Kolloquium

Kurscode: DLMMAB02

Niveau	Unterrichtssprache	SWS	ECTS	Zugangsvoraussetzungen
MA	Deutsch		1.5	Gemäß Studien- und Prüfungsordnung

Beschreibung des Kurses

Das Kolloquium wird nach Einreichung der Masterarbeit durchgeführt. Es erfolgt auf Einladung der Gutachter. Im Rahmen des Kolloquiums müssen die Studierenden unter Beweis stellen, dass sie den Inhalt und die Ergebnisse der schriftlichen Arbeit in vollem Umfang eigenständig erbracht haben. Inhalt des Kolloquiums ist eine Präsentation der wichtigsten Arbeitsinhalte und Untersuchungsergebnisse durch den Studierenden, und die Beantwortung von Fragen der Gutachter.

Kursziele

Nach erfolgreichem Abschluss sind die Studierenden in der Lage,

- eine Problemstellung aus ihrem Studienschwerpunkt unter Beachtung akademischer Präsentations- und Kommunikationstechniken vorzustellen.
- das in der Masterarbeit gewählte wissenschaftliche und methodisch Vorgehen reflektiert darzustellen.
- themenbezogene Fragen von Fachexperten (Gutachter der Masterarbeit) aktiv zu beantworten.

Kursinhalt

- Das Kolloquium umfasst eine Präsentation der wichtigsten Ergebnisse der Masterarbeit, gefolgt von der Beantwortung von Fachfragen der Gutachter durch den Studierenden.

Literatur

Pflichtliteratur

Weiterführende Literatur

- Renz, K.-C. (2016): Das 1 x 1 der Präsentation. Für Schule, Studium und Beruf. 2. Auflage, Springer Gabler, Wiesbaden.

Studienformat Fernstudium

Studienform	Kursart
Fernstudium	Thesis-Kurs

Informationen zur Prüfung	
Prüfungszulassungsvoraussetzungen	**BOLK:** Nein **Evaluation:** Nein
Prüfungsleistung	Kolloquium

Zeitaufwand Studierende					
Selbststudium	**Präsenzstudium**	**Tutorium**	**Selbstüberprüfung**	**Praxisanteil**	**Gesamt**
45 h	0 h	0 h	0 h	0 h	45 h

Lehrmethoden
Moderne Präsentationstechnologien stehen zur Verfügung.