Modulhandbuch

Cybercrime/Cybersecurity (M.Sc.)

Modulübersicht

7701 03-CCYB1	Cybercrime I
7702 03-CCYB2	Cybercrime II
7703 03-CSEO	Social Engineering und OSINT
7704 03-CGDMF	Grundlagen der Mobilfunkforensik
7705 03-CNGGS	Navigationsgeräte und Geoinformationssysteme
7706 03-CKPFM	Komplexpraktikum Forensische Methoden
7707 03-CIOT	Internet of Things
7708 03-CESFS	Embedded Systems Forensics und Speichertechnologien
7709 03-CCF	Car Forensics
7710 03-CITGO	IT-Governance
7711 03-CITC	IT-Compliance
7712 03-CSVG	Der Sachverständige vor Gericht
7713 03-STMOD	Stochastic Models
7714 03-CINT1	Computational Intelligence
7715 03-CPPDF	Predictive Policing/Dunkelfeld
7716 03-CFOMC	Foundations of Modern Cryptography
7717 03-CCA	Cryptanalysis
7718 03-CDWUG	Digitale Werte und Güter
7719 03-CDP	Datenbankprogrammierung
7720 03-CSPR	Softwarepraktikum
7721 03-CESS	Entwurf sicherer Systeme
7722 03-CDNCF	Datennetze/ Cloud Forensik
7723 03-CDKPR	Datenkompression
7724 03-CINVI	Intelligente Videoanalyse
7701 03-CCYB1	Cybercrime I
7702 03-CCYB2	Cybercrime II
7703 03-CSEO	Social Engineering und OSINT
7704 03-CGDMF	Grundlagen der Mobilfunkforensik
7705 03-CNGGS	Navigationsgeräte und Geoinformationssysteme
7706 03-CKPFM	Komplexpraktikum Forensische Methoden
7707 03-CIOT	Internet of Things
7708 03-CESFS	Embedded Systems Forensics und Speichertechnologien
7709 03-CCF	Car Forensics
7710 03-CITGO	IT-Governance
7711 03-CITC	IT-Compliance
7712 03-CSVG	Der Sachverständige vor Gericht
7713 03-STMOD	Stochastic Models
7714 03-CINT1	Computational Intelligence
7715 03-CPPDF	Predictive Policing/Dunkelfeld
7716 03-CFOMC	Foundations of Modern Cryptography
7717 03-CCA	Cryptanalysis
7718 03-CDWUG	Digitale Werte und Güter
7719 03-CDP	Datenbankprogrammierung
7720 03-CSPR	Softwarepraktikum
7721 03-CESS	Entwurf sicherer Systeme
7722 03-CDNCF	Datennetze/Cloud Forensics

Modulübersicht

7723 03-CDKPR	Datenkompression
7724 03-CINVI	Intelligente Videoanalyse
7725	Masterprojekt

Hinweis zur Bestellung der Prüfer:

Die in dem Modulhandbuch genannten Verantwortlichen werden für die jeweilige Modulprüfung zum Prüfer bestellt.

Formen für Prüfungsvorleistungen (PVL) und Prüfungssleistungen (PL):

A = alternativ, AP = Arbeitsprobe, B = Beleg, BA = Bachelorarbeit, K = Kolloquium, LA = Laborarbeit, LB = Laborbericht, LT = Labortestat, M = mündlich, ME = Medienproduktion, PA = Projektarbeit, PB = Praxisbericht, PT = Präsentation, S = schriftlich, SA = Studienarbeit, T = Testat, TM = Testat mündlich, TS = Testat schriftlich, U = Übung, V = Vortrag, R = Referat, ZD = Zeichnungsdokumentation

Modulname:	**Cybercrime I**	*Sprache:*	*deutsch*
Modulnummer:	7701	*Abschluss:*	M.Sc.
Modulcode:	03-CCYB1	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1

Ausbildungsziele:	Straftaten im Phänomenbereich Cybercrime stellen eine wachsende Herausforderung für die Strafverfolgungsbehörden in Deutschland dar. Die bloße Anzahl solcher Straftaten nimmt jährlich zu (vgl. Bundeslagebild Cybercrime) und gleichzeitig steigt der technische Aufwand bei der Begehung solcher Straftaten ständig. Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten sowie Straftaten die mittels dieser Informationstechnik begangen werden. Im Modul Cybercrime I soll auf die sogenannte IuK-Kriminalität im engeren Sinne (Computerkriminalität) eingegangen werden. Die entsprechenden Gesetzesnormen werden vorgestellt und Begehensweisen für die einzelnen Delikte erläutert. Es wird ein besonderer Augenmerkt auf die Kriminalistik gelegt. Zu den einzelnen Begehensweisen werden Kriminalstrategie und Kriminaltaktik dargelegt. Nach Abschluss des Moduls kennen die Studierenden alle relevanten Gesetzesnormen und Begehensweisen. Sie können selbstständig effiziente Ermittlungsansätze für solche Fälle entwerfen und eigenständig aufklären. Gegen Ende des Moduls wird auf die Bedeutung der Computerkriminalität im internationalen Kontext eingegangen und internationale Normen und Verfahren dargelegt.
Lehrinhalte:	IuK Kriminalität im engeren Sinne: ● Computerbetrug (§ 263a StGB) ● Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung (§§ 269, 270 StGB) ● Datenveränderung (§ 303a) ● Computersabotage (§ 303b StGB) ● Ausspähen von Daten (§ 202a StGB) ● Abfangen von Daten (§ 202b StGB) ● Softwarepiraterie: Herstellen, Überlassen, Verbreiten oder Verschaffen von sog. "Hacker-Werkzeugen", die illegalen Zwecken dienen (§ 202c StGB) Cybercrime im Internationalen Kontext ● Die EU-Cybercrime Richtlinie ● Computer Fraud and Abuse Act und Nachfolgende Regelungen in Vereinigten Staaten ● Zwischenstaatliche Vereinbarungen, G8, UN, ITU
Lernmethoden:	Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten ausgewählte Fälle aus dem Phänomenbereich Cybercrime. Für das Selbststudium werden konkrete Anregungen gegeben.
Literatur:	● Dieter Kochheim: Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik. C.H.Beck, 2015 ● Michael Büchel, Peter Hirsch: Internetkriminalität: Phänomene-Ermittlungshilfen-Prävention (Grundlagen der Kriminalistik, Band 48). Kriminalistik, 2014. ● BKA, Cybercrime: Bundeslagebild (jährlich neu) ● Chuck Easttom, Jeff Taylor: Computer Crime, Investigation, and the Law. Cengage Learning PTR, 2010. ● United Nations: Comprehensive Study on Cybercrime. 2013 ● ITU: Understanding cybercrime: Phenomena, challenges and legal response. 2012
Dozententeam:	Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine

Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7701 Cybercrime I	2	0	2	0		S 90	1/24	5

Modulname:	**Cybercrime II**	*Sprache:*	*deutsch*
Modulnummer:	7702	*Abschluss:*	M.Sc.
Modulcode:	03-CCYB2	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2

Ausbildungsziele:	Straftaten im Phänomenbereich Cybercrime stellen eine wachsende Herausforderung für die Strafverfolgungsbehörden in Deutschland dar. Die bloße Anzahl solcher Straftaten nimmt jährlich zu (vgl. Bundeslagebild Cybercrime) und gleichzeitig steigt der technische Aufwand bei der Begehung solcher Straftaten ständig. Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten sowie Straftaten die mittels dieser Informationstechnik begangen werden. Im Modul Cybercrime II soll auf die sogenannte IuK-Kriminalität im weiteren Sinne (Tatmittel Internet) eingegangen werden. Die entsprechenden Gesetzesnormen werden vorgestellt und Begehensweisen für die einzelnen Delikte erläutert. Es wird ein besonderer Augenmerkt auf die Kriminalistik gelegt. Zu den einzelnen Begehensweisen werden Kriminalstrategie und Kriminaltaktik dargelegt. Nach Abschluss des Moduls kennen die Studierenden relevante Gesetzesnormen und Begehensweisen. Sie können selbstständig effiziente Ermittlungsansätze für solche Fälle entwerfen und eigenständig aufklären.
Lehrinhalte:	IuK Kriminalität im weiteren Sinne: • Verbreitung pornographischer Schriften (Kinderpornographie) über das Internet • Verbreitung von Gewaltdarstellungen im Internet • Onlinemarktplätze (Drogenhandel, Waffenhandel, Menschenhandel) • Urheberrechtsdelikte Cybercrime im Staatsschutz • Internetdelikte PMK Rechts • Internetdelikte PMK Links • Internetdelikte PMK Islamismus Einsatz von IuK in der Organisierten Kriminalität • Geldwäsche im Internet • Bedeutung von IuK für grenzüberschreitende Kriminalität • Fälschungen IuK im Strafverfahren • IuK als falsche Beweise
Lernmethoden:	Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten ausgewählte Fälle aus dem Phänomenbereich Cybercrime. Für das Selbststudium werden konkrete Anregungen gegeben.
Literatur:	• Gerrit Manssen, Jörg Fritzsche, Robert Uerpmann-Wittzack: Strafrechtliche Verantwortlichkeit der Informationsvermittler im Netz. LIT, 2006 • Philip Jenkins: Beyond Tolerance: Child Pornography. NYU Press, 2001. • Jörg Kinzig: Die rechtliche Bewältigung von Erscheinungsformen der Organisierten Kriminalität, Berlin, 2004. • Sean S. Costigan, Jake Perry: Cyberspaces and Global Affairs. Routledge, 2012. • Bösche, Andreas: Rechtsextremismus im Internet. Schattenseiten des www. Hall 2001 • Rüdiger Quedenfeld, Udo Mühlroth, Martin Plischke, Marc Studer: Handbuch Bekämpfung der Geldwäsche und Wirtschaftskriminalität. ESV, 2013.
Dozententeam:	Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7702 Cybercrime II	2	0	2	0		S 90	1/24	5

Modulname:	**Social Engineering und OSINT**	*Sprache:*	*deutsch*
Modulnummer:	7703	*Abschluss:*	M.Sc.
Modulcode:	03-CSEO	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:	Die Studierenden verfügen über Wissen zu den Grundlagen von Social Engineering. Sie sind mit gängigen Techniken vertraut und kennen die psychologischen Grundlagen der einzelnen Angriffsmuster. Sie kennen Abwehrstrategien gegen Social Engineering und sind in der Lage Sicherheitsrichtlinien und Schulungen zu entwickeln. Jeder Teilnehmer kennt die Möglichkeiten von OSINT (Open Source Intelligence) zur Datengewinnung. ER kann selbstständig Werkzeuge einsetzen um Daten automatisiert zu sammeln, zusammenzuführen und auszuwerten. Dabei wird er mit den Besonderheiten von Big Data konfrontiert. Alle Kursteilnehmer sind vertraut der Daten Gewinnung aus Sozialen Netzwerken, Webseiten, Medien und anderen offenen Quellen. Sie lernen Personen zu identifizieren und zu lokalisieren.
Lehrinhalte:	Grundlagen des Social Engineering • Reziprozität • Konsistenz • Commitement Andrere Techniken • Phishing • Dumpster Diving Abwehrstrategien gegen Social Engineering Grundlagen von OSINT • Arten von offenen Quellen • Automatisiertes Sammeln von Informationen • Zusammenführen von Informationen • Auswertung offener Quellen • Big Data
Lernmethoden:	Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten an ausgewählte Problemen aus dem Bereich Social Engineering und OSINT. Diese werden vertiefend diskutiert und typisch Strategien und Angriffsmuster an Beispielszenarien aufgezeigt. Für das Selbststudium werden konkrete Anregungen gegeben.
Literatur:	• Kevin D. Mitnick, William L. Simon: Die Kunst der Täuschung. Risikofaktor Mensch. mitp, Heidelberg 2006 • Cialdini, R. B.: Die Psychologie des Überzeugens. Verlag Hans Huber, 2007. • Stefan Schumacher: Psychologische Grundlagen des Social Engineering. In: Die Datenschleuder. 94, 2010 • Arthuer S. Hulnick: 'The Dilemma of Open Source Intelligence: Is OSINT Really Intelligence?', pages 229-241, The Oxford Handbook of National Security Intelligence, 2010 -Andreas Weyert : Hacking mit Kali. Francis, 2014.
Dozententeam:	Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher) M.Sc. Spranger, Michael
Voraussetzungen:	keine
Vorausges. Module:	keine

Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7703 Social Engineering und OSINT	1	0	3	0	LT	M 30	1/24	5

Modulname:	**Grundlagen der Mobilfunkforensik**	*Sprache:*	*deutsch*
Modulnummer:	7704	*Abschluss:*	M.Sc.
Modulcode:	03-CGDMF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1

Ausbildungsziele:	Weltweit existieren über 6 Mrd. Mobilfunknutzer, dies macht mehr als 90% der Weltbevölkerung aus. Bereits im Jahr 2013 waren in 85% aller Kriminalfälle mobile Endgeräte involviert. Trotz der stetig wachsenden Bedeutung mobiler Endgeräte wie Mobiltelefonen, Smart-Phones, PDAs und Musikgeräten gilt die forensische Untersuchung solcher Geräte als teuer und kompliziert. Im Modul "Grundlagen der Mobilfunkforensik" sollen verbreitete Mobilfunkstandards, Betriebssysteme und Grundlagen der Architektur von mobilen Endgeräten strukturiert dargestellt werden. In einem zweiten Teil sollen forensische Tools für mobile Endgeräte vorgestellt und Szenarien erörtert werden. Nach Abschluss des Moduls sollen die Studierenden Kompetenzen im Bereich Mobilfunkforensik der Art erworben haben, dass sie selbstständig in der Lage sind derart gelagerte Spurenträger zu untersuchen.
Lehrinhalte:	• Mobilfunksysteme: Mobilfunksysteme und Mobilfunkstandards der 2. bis 4. Generation (GSM, GPRS, UMTS, LTE), Frequenzbereiche und Frequenzregulierung, Grundlagen zellularer Mobilfunksysteme, Systemeigenschaften (Sendeleistungen, Datenraten, Übertragungsbandbreiten, usw.), Netzwerkarchitekturen und Systemkomponenten, Adressen und Kennziffern zum Auffinden eines Teilnehmers, Luftschnittstelle (Medienzugriffs- und Übertragungsverfahren, Kanalstrukturen), Mobilitätsmanagement, IT-Sicherheit. Mobilfunkforensik: • Grundlagen und Begriffe der Mobilfunkforensik • Smartcards: insbesondere SIM • Mobile Betriebssysteme: insbesondere Android, iOS, WindowsPhone • Architektur von Mobilfunkendgeräten: insbesondere Speichertechnologien • Forensische Tools: insbesondere UFED, XRY • Der IMSICatcher
Lernmethoden:	Im Rahmen des Masterstudiums werden Vorlesungen mittels Beamer-Präsentationen und Tafel gehalten, in denen wichtige theoretische und praxisrelevante Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Fallbeispielen werden Herangehensweisen an definierte Mobilfunkendgeräte sowie mögliche Lösungsstrategien erörtert. Im Praktikum werden ausgewählte Aufgabenstellungen am Spurenträger praktisch verwirklicht. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt.
Literatur:	• Satish Bommisetty, Rohit Tamma, Heather Mahalik: Practical Mobile Forensics. Packt Publishing 2014. • Wolfgang Rankl, Wolfgang Effing: Handbuch der Chipkarten: Aufbau - Funktionsweise - Einsatz von Smart Cards. 5. Auflage, Hanser, 2008. • Bernhard Walke: Mobilfunknetze und ihre Protokolle 1, Stuttgart 2001, ISBN 3-519-26430-7. • Jonathan Zdziarski : iOS Forensic Investigative Methods, 2012. M. Sauter, Grundkurs Mobile Kommunikationssysteme, Springer, 6. Aufl., 2015, ISBN-13: 978-3658083427. C. F. Lüders, Mobilfunksysteme, Vogel, 2001, ISBN-10: 3802318471. J. Hoy, Forensic Radio Survey Techniques for Cell Site Analysis, John Wiley & Sons, 2015, ISBN 9781118925737.
Dozententeam:	Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher) Prof. Dr.-Ing. Delport, Volker
Voraussetzungen:	keine
Vorausges. Module:	keine

Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7704 Grundlagen der Mobilfunkforensik	2	1	1	0		S 90	1/24	5

Modulname:	**Navigationsgeräte und Geoinformationssysteme**	*Sprache:*	*deutsch*
Modulnummer:	7705	*Abschluss:*	M.Sc.
Modulcode:	03-CNGGS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2

Ausbildungsziele:

Navigationsgeräte sind heutzutage in nahezu jedem Haushalt zu finden. Mit Hilfe dieser technischen Systeme erfolgt eine Positionsbestimmung und durch Verwendung von Geoinformationen wie Topologie-, Straßen-, Luft- oder Seekarten dementsprechend die Berechnung der zielführenden Fahrtrouten. Im Modul "Navigationsgeräte und Geoinformationssysteme" sollen die Navigationsstandards, einzelne Systeme und Grundlagen der Geoinformatik strukturiert dargestellt sowie Fundamente der geographischen Informationssysteme näher gebracht werden.

Lehrinhalte:

- Geodäsie und Kartographie,
- Satellitennavigation,
- Spatial Data,
- Implementierung und Nutzung von Geoinformationssystemen

Lernmethoden:

Im Rahmen des Moduls finden Vorlesungen und Seminare statt. In den Vorlesungen werden die Prinzipien und Grundlagen von Navigationsgeräte und Geoinformationssystemen definiert und vorgestellt. Es werden wichtige theoretische und praxisrelevante Inhalte vermittelt sowie ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Die Vorlesung erfolgt mittels Beamer-Präsentationen und Tafelanschrieb.

Die Vertiefung der Kenntnisse und Lehrinhalte erfolgt im Seminar. Anhand konkreter Fallbeispiele werden Herangehensweisen an definierte Geoinformationssysteme sowie ausgewählte Navigationsgeräte erörtert.

Literatur:

- Kahl W.: Navigation für Expeditionen, Touren, Törns und Reisen: Orientierung in der Wildnis, Schettler, 1991
- R Kothuri, A Godfrind, E Beinat: Pro oracle spatial for oracle database 11g, Dreamtech Press, 2008
- Linke W.: Orientierung mit Karte, Kompaß, GPS, Delius Klasing, 2008
- Longley P., et al.: Geographic Information System and Science, UNIGIS Amsterdam, 2001
- Schönfeld R.: Das GPS Handbuch. GPS-Handgeräte in der Praxis: Grundlagen, Basis-Funktionen, Navigation und Orientierung, Karten, Band 1 und 2, Monsenstein und Vannerdat, 2008
- Umland H.: A Short Guide to Celestial Navigation, 1997

Dozententeam:

Prof. Dr. rer. biol. hum. Stübner, Rudolf (Hauptverantwortlicher)

Voraussetzungen:

Vorausgesetzt werden fundierte Kenntnisse der Programmierung (Java) sowie Grundlagen im Umgang mit Datenbanken (SQL).

Vorausges. Module:

keine

Arbeitslast: *- workload*

150 Stunden, davon
60 Stunden Lehrveranstaltungen
90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7705 Navigationsgeräte und Geoinformationssysteme	2	2	0	0		PA	1/24	5

Modulname:	**Komplexpraktikum Forensische Methoden**	*Sprache:*	*deutsch*
Modulnummer:	7706	*Abschluss:*	M.Sc.
Modulcode:	03-CKPFM	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:

Die Studierenden lernen in selbstgewählten Modulen praktische Verfahrensweisen aus dem Bereich Cybercrime / Cybersecurity kennen. In den einzelenen Praktika sollen die Studierenden erlernen Ihre im Studium erworbenen Fähigkeiten einzusetzen und selbst gewählte Spezialgebiete vertiefen.

Lehrinhalte:

Auswahl bis zu 2 Praktika aus:

- Forensische Digitalfotographie
- Sicherheitsmerkmale bei Wertzeichen und Urkunden
- Open Source Intelligence
- Malware Forensics
- Digitale Audioanalyse
- Methoden der Digitalen Tatortrekonstruktion
- Car Forensics
- Digitale Fallanalyse
- Digital Video Analysis
- Mobilfunkforensik

(Die Module werden entsprechend der Fortschritte der IT-Forensik aktualisiert.)

Lernmethoden:

Die Komplexpraktika finden an der Hochschule Mittweida statt. Hier sollen die theoretische Grundlagen der Studierenden zu Anwendung kommen. In diesem Zusammenhang werden ausgewählte Probleme vertiefend in Vorlesungen und Seminaren diskutiert und Strategien zur Problemlösung vorgestellt. Dann sollen die Studierenden konkrete Problemen in Kleingruppen praktisch lösen.

Literatur:

Die Literaturempfehlungen richten sich nach den gewählten Einzelpraktika im Rahmen des Komplexpraktikums.

Dozententeam:

Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher)
Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher)

Voraussetzungen:

keine

Vorausges. Module:

keine

Arbeitslast: *- workload*

150 Stunden, davon
60 Stunden Lehrveranstaltungen
90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7706 Komplexpraktikum Forensische Methoden	0	2	2	0			1/24	5
7706(T1) Teilprüfung 1						LB		
7706(T2) Teilprüfung 2						LB		

Modulname:	**Internet of Things**	*Sprache:*	*deutsch*
Modulnummer:	7707	*Abschluss:*	M.Sc.
Modulcode:	03-CIOT	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1

Ausbildungsziele:	Vermittlung von Kenntnissen über die Vernetzung und die Bestandteile des Internets der Dinge - Internet of Things. Ausgehend von einzelnen Komponenten wie RFID-Systeme, Sensoren, Aktoren, Embedded Systeme wird die vernetzte Kommunikation über das Internet demonstriert. Die Studierenden erwerben Wissen bezüglich des Aufbaus, der Funktionsweise und der Implementierung von IoT Anwendungen in Hard- und Software.
Lehrinhalte:	• Einführung in das Internets der Dinge (IoT) • Protokolle und Technologien • Sensoren, Aktoren und deren Funktionsprinzip und Anschluss • RFID-Systeme in Hard- und Software • Mikrocontroller und TCP/IP Stack als Kommunikationsendpunkte • Datenkommunikation über das Internet mit embedded Systemen und angeschlossenen Sensoren und Aktoren • Wireless Sensor Network Technologie-Funksensoren IEEE 802.15.4
Lernmethoden:	• Vorlesungen, Beamer-Präsentationen, Tafel; • Übungen und Praktika im Computerpool, Präsentation
Literatur:	• Tanenbaum, A.: Computernetzwerke, International Edition 2011 • Meyer, Martin: Kommunikationstechnik:, Vieweg +Teubner Verlag GmbH, 2011 ISBN 978-3-8348-1338-1 • Tietze, U.; Schenk, Ch.: Halbleiter-Schaltungstechnik. - Springer Verlag: Berlin Heidelberg New York u.a. - ISBN 3-540-56184-6 • www.Keil.com - uVison4/5 und 32 Bit ARM-Controller LPC1768 Dokumentation, 2014
Dozententeam:	Prof. Dr. Dr.-Ing. Luge, Hartmut (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 75 Stunden Lehrveranstaltungen 75 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7707 Internet of Things	2	2	1	0		A	1/24	5

Modulname:	**Embedded Systems Forensics und Speichertechnologien**	*Sprache:*	*deutsch*
Modulnummer:	7708	*Abschluss:*	M.Sc.
Modulcode:	03-CESFS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2

Ausbildungsziele:

Klassische PCs verschwinden zunehmend als Gerät und werden durch "intelligente Gegenstände" ersetzt. Immer kleinere embedded Systems übernehmen Aufgaben, ohne dass ihre Existenz in jedem Fall überhaupt bekannt wird. So werden miniaturisierte Computer, zum Beispiel als sogenannte Wearables, mit unterschiedlichen Sensoren direkt in Kleidungsstücke eingearbeitet. Auch der klassische Magnetspeicher verschwindet zunehmend und wird durch elektronische Flash Speicher ersetzt. Diese Entwicklung stellt ganz neue Herausforderungen an die IT-Forensik und wird zu bedeutenden Umwälzungen führen.

Im Teil "Embedded Systems Forensics" sollen verbreitete Technologien und Standards, Betriebssysteme und Grundlagen der Architektur von eingebetteten Systemen strukturiert dargestellt werden. Im Praktikum sollen Embeddeds eigenständig programmiert und ausgewertet werden. Im zweiten Teil "Speichertechnologien" sollen die Grundlagen moderner Speichertechnologien vermittelt werden. Es werden forensischen Tools für die Auswertung von eingebetteten Systemen vorgestellt und Szenarien erörtert.

Nach Abschluss des Moduls sollen die Studierenden Kompetenzen im Bereich Embbeded Systems der Art erworben haben, dass sie selbstständig in der Lage sind derart gelagerte Spurenträger zu untersuchen.

Lehrinhalte:

- Grundlagen und Begriffe eingebetteter Systeme
- typische Realisierungen - Mikrocontroller und FPGA (Grundaufbau, mbed-Standard, Beispiele)
- Programmiermethoden und Beobachtbarkeit (JTAG, Busanalysator, ...)
- RFID
- Flash-Technologien: NAND-Flash, NOR-Flash, EMMCs
- AT-Befehle bei Speichermedien

Lernmethoden:

Die Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im Seminar werden ausgewählte Probleme eingehender diskutiert. Im betreuten Praktikum bearbeiten die Studenten ausgewählte Probleme aus dem Bereich Embedded Systems Forensics und Speichertechnologien. Für das Selbststudium werden konkrete Anregungen gegeben. Anhand von konkreten Fallbeispielen werden Herangehensweisen an definierte Embeddeds sowie mögliche Lösungsstrategien erörtert.

Literatur:

- John Catsoulis: Designing Embedded Hardware. O'Reilly, 2005.
- Paolo Pavan, Roberto Bez, Piero Olivo, Enrico Zanoni: Flash Memory Cells - An Overview. IEEE 1997
- Klaus Finkenzeller: RFID Handbuch.Hanser 2008
- Niklaus Wirth: Digital Circuit Design An Introduction Textbook. Springer, 1995
- IEEE STd 1149.1 (JTAG) Testability Primer, Texas Instruments, 1997

Dozententeam:

Voraussetzungen: keine

Vorausges. Module: keine

Arbeitslast: *- workload*

150 Stunden, davon
60 Stunden Lehrveranstaltungen
90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7708 Embedded Systems Forensics und Speichertechnologien	2	1	1	0		B	1/24	5

Modulname:	**Car Forensics**	*Sprache:*	*deutsch*
Modulnummer:	7709	*Abschluss:*	M.Sc.
Modulcode:	03-CCF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:	Die Digitalisierung von Kraftfahrzeugen schreitet stetig voran. Neben elektronischen Steuergeräten, die in modernen Fahrzeugen verbaut sind, entstehen in Themenfeldern wie Car2Car-, Car2Infrastructure und Car2Person-Kommunikation neue Felder, die eine Spezialisierung der elektronischen Forensik in den Bereich Car Forensics unabdingbar machen. Trotz der stetig wachsenden Bedeutung von Kfz für die Kriminalistik die forensische Untersuchung von Fahrzeugen als teuer und kompliziert. Im Modul "Car Forensics" sollen verbreitete Standards, Bussysteme und Grundlagen der Architektur von Steuergeräten in Kfz strukturiert dargestellt werden. In einem zweiten Teil sollen forensische Tools für Fahrzeuge vorgestellt und Szenarien erörtert werden. Nach Abschluss des Moduls sollen die Studierenden Kompetenzen im Bereich Car Forensics der Art erworben haben, dass sie selbstständig in der Lage sind derart gelagerte Spurenträger zu untersuchen.
Lehrinhalte:	• Bussysteme: CAN, LIN, K-Line • Grundlagen und Begriffe der Car Forensics • Steuergeräte: insbesondere Funktion von Wegfahrsperren • Kfz-Untersuchungen • Architektur von Kfz, insbesondere Fahrzeugelektronik • Forensische Tools • Car2Car-, Car2Infrastructure und Car2Person-Kommunikation
Lernmethoden:	Das Seminar vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel in kleinen Gruppen. An Beispielen sollen die Studierenden mit der Materie vertraut gemacht werden. Im betreuten Praktikum sollen die Studenten eigenständig Datensicherungen an Kraftfahrzeugen durchführen und die gewonnenen Daten selbstständig auswerten. Im Seminar werden ausgewählte Themen vertieft und Aufgaben gemeinsam erarbeitet. Für das Selbststudium werden konkrete Anregungen gegeben.
Literatur:	In dem jungen Forschungsfeld haben sich noch keine Standardwerke etabliert. Die Studierenden erhalten Skripte und aktuelle Forschungsergebnisse im Seminar. • Thomas Käfer: Car-Forensics. Books on Demand, 2015.
Dozententeam:	Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7709 Car Forensics	0	2	2	0	PA	M 30	1/24	5

Modulname:	**IT-Governance**	*Sprache:*	*deutsch*
Modulnummer:	7710	*Abschluss:*	M.Sc.
Modulcode:	03-CITGO	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1

Ausbildungsziele:	Ziel ist es, die Studenten nach erfolgreichem Abschluss dieses Moduls zu befähigen, Führungsverantwortung zu vermitteln und Organisationseinheiten mit Informatikschwerpunkt zu übernehmen. ● Sie verstehen die Zusammenhänge von Organisation und IT-Systemen als Teil der strategischen Unternehmensplanung und -organisation, ● Die Studenten sind in der Lage IT-Systeme als Werkzeug für das Erreichen der Unternehmensziele zu verwenden, ● Sie gewinnen an Erfahrung in Planung und Organisation der Informationsver-arbeitung, ● Das erworbene Wissen kann zu Unternehmensführung unter Berücksichtigung von Erfolgsfaktoren wie z.B. Qualität, Nachhaltigkeit, Unternehmenserfolg dienen.
Lehrinhalte:	● Unternehmensziele und kritische Erfolgsfaktorendes IT-Managements zu erkennen um umzusetzen. ● Erkennen von Wettbwerbsvorteilen und damit Kernkompetenzen und Kernprozes-sen und Ermittlung der entsprechenden Schlüsselinformationen, ● Planung und Aufbau einer IT-Infrastruktur, Entscheidungskriterien und -prozesse, Entwicklungsmodelle ● IT-Controlling, Kosten-/ Nutzenanalyse, Portfoliomanagement ● Organistionoptionen für das Informationsmanagement, ZB. Eigenentwicklung, Stanardsoftware, In- und Outsourcing, Cloud, Software as a Service ● Qualitätsmanagement nach aktuellen Standards, z.B. CMM, Total Quality Management, ISO-Standards
Lernmethoden:	Vorlesung und Seminar
Literatur:	● Balzert, H.: Lehrbuch der Software- Technik 1/2. mit 3 CD-ROMs. Band 1, Band 2 Software- Entwicklung / Software-Management, Software- Qualitätssiche-rung, Unternehmensmodellierung; Spektrum-Verlag, ● Berg, Björn et al.: Hybride Softwareentwicklung Das Beste aus klassischen und agilen Methoden in einem Modell vereint; Springer, Heidelberg, 2014 ● BSI (Bundesamt für Sicherheit in der Informationstechnik): IT-Grundschutz ● Buchanan, David A.; Huczynski, Andrzej A.: Organizational Behaviour, 7th ed., Pearson Education, Harlow, UK; 2012. ● Burghardt, M.: Projektmanagement - Leitfaden für die Planung, ● Überwachung und Steuerung von Entwicklungsprojekten; Siemens Verlag: Berlin; 2012. ● Gadatsch, A.: Masterkurs IT-Controlling; Vieweg-Verlag, Wiesbaden, ● Helmke, Stefan, Uebel, Matthias: Mangementorientiertes IT-Controlling und IT-Governance, Springer-Heidelber, 2016, DOI: 10.1007/978-3-658-07990-1. ● Krcmar, H: Informationsmanagement; Springer-Verlag, Berlin ● Schmidt, Götz: Organisation und Business Analysis - Methoden und Techniken, Verlag Götz Schmidt, Wettenberg (bzw. Auch bei der Gesellschaft für Projektma-nagement wieder zu finden) ● Schneider, Kurt: Abenteuer Softwarequalität: Grundlagen für Qualitätssicherung und Qualitätsmanagement, dpunkt-Verlag, ● Suicimezov, Natalia ; Georgescu, Mircea Radu: IT-Governance in Cloud Procedia Economics and Finance, 2014, Vol.15, pp.830-835 [Peer Reviewed Jour-nal, ● Wöhe, Günther; Döring, Urlich: Einführung in die allgemeine Betriebswirt- ● schaftslehre; Verlag Vahlen; München ● Zeitschriften:

	• BISE business & information systems engineering • European Journal of information Systems (EJIS) • Information Management (I & M) ISSN: 0378-7206) • Praxis der Wirtschaftsinformatik: http://hmd.dpunkt.de/ • Information & management • Informatik Spektrum • International journal of information management • International journal of productivity and quality management • Journal of enterprise information management • IT-Governance • Management information systems • Quality management journal
Dozententeam:	Prof. Dr. rer. pol. Schmidt, Petra (Hauptverantwortlicher)
Voraussetzungen:	Für dieses Modul werden Informatikkenntnisse vorausgesetzt, die in einem Bachelor-studiengang der (angewandten) Informatik oder verwandten Studiengang vermittelt werden. Darüberhinaus wird die Kenntnis wissenschaftlichen Arbeitens vorausgesetzt.
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7710 IT-Governance	2	2	0	0		S 90	1/24	5

Modulname:	**IT-Compliance**	*Sprache:*	*deutsch*
Modulnummer:	7711	*Abschluss:*	M.Sc.
Modulcode:	03-CITC	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2

Ausbildungsziele:	Bachelorstudium in der IT-Forensik und IT-Sicherheit und verwandten Studiengängen. Die Studenten sind nach erfolgreichem Abschluss dieses Moduls in der Lage Führungsverantwortung in Organisationseinheiten mit Informatikschwerpunkt zu übernehmen. ● Die Studenten erhalten einen Überblick über die exogenen Einflüsse auf das IT-Management. ● Das erworbene Wissen kann zur Unternehmensführung unter Berücksichtigung von Erfolgsfaktoren wie z.B. Gesetzeslage, Standards, etc dienen ● organisatorische Voraussetzung zur Gewährleistung der IT-Sicherheit ● Nachhaltigkeit, Unternehmenserfolg.
Lehrinhalte:	● Die Studenten lernen die wesentlichen Inhalte der ISO 27000 kennen. ● Sie erwerben Kenntnisse über die Etablierung effektiver Informationssicherheit. ● Anwendung von Methoden und Instrumente der IT-Prüfung, und der IT-Revision an ● Kenntniserwerb in Datenschutz und Datenschutzaudit ● Erwerb der Fähigkeit mit Interessenkonflikten wie z.B. Data Mining versus Datenschutz umzugehen. ● Studenten lernen proaktiv zu denken und zu handeln, um Verstöße gegen unternehmensbezogene Rechtsvorschriften durch angemessene Aufsichts- und Überwachungsmaßnahmen zu verhindern (vgl. etwa §30 OWiG) ● Befähigung zu einer IT Revision bei Betrugsaufdeckung durchzuführen -Erlernen von Grundzügen des Risiko-Managements
Lernmethoden:	Vorlesung und Seminar
Literatur:	● Ahn, Heinz et al.: Steuerung von IT-Compliance-Management-Systemen in Kon-zern-Strukturen, in: HMD Praxis der Wirtschaftsinformatik, 2014, Vol.51(3), p.240; DOI: 10.1365/s40702-014-0028-x. ● CoBiT ● Compliance Manager, ● Emmert, Ulrich: Europäische und nationale Regelungen, in : Datenschutz und Datensicherheit - DuD, 2016, Vol.40(1), pp.34-37. DOI: 10.1007/s11623-016-0539-4. ● Helmke, Stefan, Uebel, Matthias: Mangementorientiertes IT-Controlling und IT-Governance, Springer-Heidelber, 2016, DOI: 10.1007/978-3-658-07990-1. ● Lissen, Nina et al.: IT-Services in der Cloud und ISAE 3402 - Ein praxisorientierter Leitfaden für eine erfolgreiche Auditierung, Springer, Gabler, 2014. ● ISO17021 und ISO 19011 Leitfäden zur Auditierung bzw. Zertifizierung von Managementsystemen ● ISO 27000 IT-Sicherheit ● Boris Koppenhöfer: Grundlagen Datenschutz - Eine Information für Beschäftigte; Books on Demand, 2015. ● Krupna, Carsten: Informationspflichten nach dem Bundesdatenschutzgesetz bei einem Hackerangriffen, in: Betriebs-Berater, 2014(38), p.2250 2251 2252 2253 2254. ● OWiG (Gesetz über Ordnungswidrigkeiten):IT-Compliance: Erfolgreiches Ma-nagement regulatorischer Anforderungen, Erich-Schmidt.Verlag, 2014. ● Publikationen der Deutschen Gesellschaft für Recht in der Informatik ● Sowa, Aleksandra et al.: IT-Revision, IT-Audit und IT-Compliance, Springer, Heidelberg, 2015, ISBN: 978-3-658-02807-7 ● Zeitschriften: ● IT-Governance

Dozententeam:	Prof. Dr. rer. pol. Schmidt, Petra (Hauptverantwortlicher)
Voraussetzungen:	Voraussetzung von Informatikkenntnissen. Darüberhinaus wird die Kenntnis wissenschaftlichen Arbeitens vorausgesetzt und Kenntnisse des Moduls IT-Governance vorausgesetzt.
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7711 IT-Compliance	2	2	0	0		S 90	1/24	5

Modulname:	**Der Sachverständige vor Gericht**	*Sprache:*	*deutsch*
Modulnummer:	7712	*Abschluss:*	M.Sc.
Modulcode:	03-CSVG	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:

IT-Forensiker wie Ermittler müssen die Ergebnisse Ihrer Arbeit in Gutachten darlegen. An solche Gutachten werden definierte formale Ansprüche gestellt. Auch müssen diese Gutachten vor Gericht vertreten werden, auch hier gibt es einen formalen Rahmen der einzuhalten ist. Neben den formalen Kriterien gibt es eine Menge ungeschriebene Gesetze einzuhalten und der Sachverständige soll auch rhetorisch überzeugen.

Das Modul "Der Sachverständige vor Gericht" soll die Anforderungen an ein Gutachten beziehungsweise an einen Sachverständigenvortrag vermitteln. Daneben sollen sprachliche und rhetorische Besonderheiten im Strafprozess dargelegt werden.

Lehrinhalte:

- Das Sachverständigengutachten
- Der Sachverständigenvortrag
- Der Sachverständige in der StPO
- Juristische Rhetorik
- Sprache und Duktus des Sachverständigenvortrags

Lernmethoden:

In der Vorlesung werden wichtige theoretische und praxisrelevante Grundlagen vermittelt. Im Seminar werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand eines konkreten Falls soll eigenständig ein Gutachten geschrieben und ein Sachverständigenvortrag vorbereitet werden. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Das Erstellte Gutachten soll in einem Sachverständigenvortrag dargestellt werden. In einem Rollenspiel wird eine Gerichtsverhandlung nachgestellt.

Literatur:

- Walter Byerlein: Praxishandbuch Sachverständigenrecht. CH.. Beck, 2000.
- Harald Krammer, Jürgen Schille, Alexeander Schmidt, Alfred Tanczos: Sachverständige und ihre Gutachten. Manz 2015
- Fritjof Haft: Juristische Rhetorik. Alber Studienbuch, 2009.

Dozententeam:

Prof. Dr. rer. nat. Hummert, Christian

Prof. Dr. rer. nat. Labudde, Dirk

Voraussetzungen: keine

Vorausges. Module: keine

Arbeitslast: *- workload*

150 Stunden, davon
60 Stunden Lehrveranstaltungen
90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7712 Der Sachverständige vor Gericht	1	3	0	0			1/24	5
7712(T1) Teilprüfung 1						B		
7712(T2) Teilprüfung 2						K 20		

Modulname:	**Stochastic Models**	*Sprache:*	*deutsch*
Modulnummer:	7713	*Abschluss:*	M.Sc.
Modulcode:	03-STMOD	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1

Ausbildungsziele:	Das Hauptziel ist die Vermittlung fundierter Kenntnisse in Bereich der Modellbildung und stochastischen Simulation sowie deren Anwendung in statistischen Methoden. Die Studierenden lernen den Umgang mit verschiedenen Klassen von stochastischen Prozessen kennen. Praxisnahe Anwendungsbeispiele werden im Praktikumsteil am Computer implementiert. Auf diese Weise soll bei den Studierenden ein tiefgehendes Verständnis für die Modellierung stochastischer Prozesse herausgebildet werden. Studierende erlernen die Fähigkeit Probleme konzeptionell zu erfassen, zu strukturieren, zu modellieren und - insbesondere mittels stochastischer Simulation - eigenständig zu lösen. The main objective is the acquirement of solid knowledge of probabilistic modeling and stochastic simulation, as we ll as their application to statistical methods. Students learn to handle various classes of stochastic processes. Practical applications will be disc ussed in detail and implemented and solved using computerized methods. Based on that, students will gain a deep understanding of modeling stochastical processes. Additionally, students will acquire the abilities to comprehend practical problems conceptually, to structure and model them, and to independently solve them, particularly using stochastic simulations.
Lehrinhalte:	Im Modul Stochastische Modelle werden diskrete und kontinuierliche stochastische Prozesse vorgestellt, insbesondere Markovketten, Martingal-Prozesse, Geburts-Todesprozesse sowie Verzweigungs- und Koaleszenzprozesse eingegangen. Es wird insbesondere auf die Simulation von stochastischen Prozessen (z.B. MCMC) eingegangen sowie deren Anwendung in statistischen Verfahren (Bayes‘sche Verfahren, Approximativ Bayes'sche Verfahren). In this module discrete and continuous stochastic processes are introduced, in particular, Markov chains, Martingal-processes, birth-death processes, branching and coalescence processes. Particular focus lies on simulation techniques of stochastic processes (e.g. MCMC) as well as on their applications in statistical procedures (Bayesian and approximate Bayesian methods).
Lernmethoden:	Klassische Vorlesung (Präsentationen, Animationen und Illustrationen enthaltend), Übungen, studentische Vorträge in Seminaren, Bearbeitung von Aufgabenstellungen mittels Computeralgebrasystemen/ Matrizen-sprachen (z.B. Mathematica, Maple, MatLab) , statistischer Software (z.B. SAS, SPSS, R) und Programmiersprachen (Phython, C++). Classic lecture (pre sentations, animations and illustrations containing), exercises, student presentations in seminars, processing of tasks using computer algebra systems/ matrices-languages (e.g. , Mathematica, maple, Matlab), statistical software (e.g. , SAS, SPSS, R) and programming languages (Phython, C++).
Literatur:	H. Bauer: Wahrscheinlichkeitstheorie. de Gruyter, 4. Auflage (1991). P. Billingsley: Probability and measure. Wiley (1986). R. Durret: Probability theory and examples . Cambridge University Press, 4. Auflage (30. August 2010). G. Pflug: Stochastische Modelle in de r Informatik. B.G. Teubner Stuttgart, 1986. I. M. Sobol: Die Monte-Carlo-Methode, Taschenbücher Nr. 41. Harri Deutsch, Frankfurt a. M., 1985.
Dozententeam:	Prof. Dr. rer. nat. habil. Schneider, Kristan (Hauptverantwortlicher)
Voraussetzungen:	keine

Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7713 Stochastic Models	2	1	1	0		S 120	1/24	5

Modulname:	**Computational Intelligence**	*Sprache:*	*deutsch*
Modulnummer:	7714	*Abschluss:*	M.Sc.
Modulcode:	03-CINT1	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2

Ausbildungsziele:	In der Lehrveranstaltung erwerben die Studierenden Wissen über grundlegende mathematisch-algorithmische Prinzipien im maschinellen Lernen. Schwerpunkt bilden neuronale Netze und Modelle des Hebb"schen Lernens zur Mustererkennung und Klassifikation. Im Computerpraktikum erlernen die Studierenden, einfache Algorithmen in ihrem Verhalten zu modellieren und zu untersuchen. The course provides the basic principles and algorithms in CI. Particularly, neural networks for clustering and classification as well as Hebb learning are in the main focus. Completing the course, students are able to program basic models and to study their behavior.
Lehrinhalte:	Biologische Neuronen, Perzeptron, Mehrschicht-Netzwerke, Hebb"sches Lernen, Vektorquantisierung. Maschinelles Lernen mit MATLAB: Programmierung einfacher Modelle, Konvergenz. Biological neurons, perceptrons, multi-layer perceptrons , Hebbian learning, vector quantization. Machine Learning in MATLAB: programming of machine learning models in MATLAB, analysis of convergence behavior,exemplary applications.
Lernmethoden:	Kreide und Tafel, Beamer, Vorträge, Übungsaufgaben, eigene Programmierprojekte. Chalk and blackboard, slides, homework exercises, student's presentations, programming projects.
Literatur:	C. Bishop: Pattern Recognition and Machine Learning. Springer, 2007. S. Haykin: Neural Networks. Pearson Education, 2004. R. Kruse: Computational Intelligence. Teubner, 2011. H. Ritter, T. Martinetz & K. Schult en: Neural Computation and Self-Organizing Maps. Addison-Wesley, 1992. M. Mayamoto: Fuzzy Clustering. Springer 2010.
Dozententeam:	Prof. Dr. rer. nat. habil. Villmann, Thomas (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7714 Computational Intelligence	2	1	1	0		M 30	1/24	5

Modulname:	**Predictive Policing/Dunkelfeld**	*Sprache:*	*deutsch*
Modulnummer:	7715	*Abschluss:*	M.Sc.
Modulcode:	03-CPPDF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:	In der Kriminalforschung bezeichnet das Dunkelfeld die Differenz zwischen den amtlich registrierten Straftaten, dem Hellfeld, und der vermutlich begangenen Kriminalität. Allein durch die Kriminalstatistiken kann vom Hellfeld nicht auf die tatsächliche Kriminalität geschlossen werden. Daher bedarf es der Dunkelfeldforschung, um das Dunkelfeld aufzuhellen und einen systematischen Überblick über die Kriminalitätsentwicklung zu erreichen. Predictive Policing hingegen bezeichnet die Analyse von Falldaten zur Berechnung der Wahrscheinlichkeit zukünftiger Straftaten zur Steuerung des Einsatzes von Polizeikräften Nach Abschluss des Moduls können die Studierenden die amtlichen Kriminalstatistiken lesen und verstehen. Sie kennen die aktuellen Verfahren um Aussagen über das Dunkelfeld und damit über die tatsächliche Kriminalität zu treffen. Die Studierenden erhalten ein differenziertes Bild von der Möglichkeit des Predictive Policing und Aussagekraft von Aussagen über die Vorhersage von Straftaten. Sie können mit einfachen Methoden selbstständig Modelle entwickeln. Nach Abschluss des Moduls verfügen die Studierenden über einen abgerundeten Überblick über das Fachgebiet. Sie können selbstständig Modellansätze entwerfen und eigenständig berechnen.
Lehrinhalte:	• Die Polizeiliche Kriminalstatisik • Hellfeld und Dunkelfeld • Kriminalitätsmessung • Kriminalitätsanalyse und kriminalstatistische Forschung • "Ethnic Profiling" • Re-Victimisierung • Ethische Implikationen von Predicted Policing • Rational-Choice-Theorie • Boost-Hypothese • Flag-Hypothese • Near-Repeat-Victimisation • Methoden zur Vorhersage • Modellierung von Kriminalität • Extrapolationsalgorithmen • Validierung von Kriminalitätsmodellen
Lernmethoden:	Im Rahmen der seminaristischen Vorlesung werden wichtige theoretische Grundlagen vermittelt werden. In diesem Zusammenhang werden auch ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Problemen werden die Studierenden mit Herangehensweisen konfrontiert und ausgewählte Themen werden eingehend erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Im Praktikum sollen verschiedene Algorithmen aus dem Bereich Predictive Policing/Dunkelfeld in Software implementiert werden.
Literatur:	• Uwe Dörmann, Wolfgang Heinz: Zahlen sprechen nicht für sich. Aufsätze zu Kriminalstatistik, Dunkelfeld und Sicherheitsgefühl aus drei Jahrzehnten. Luchterhand, 2004. • Thomas Feltes, Benjamin Schmidt: Policing Diversity: Über den Umgang mit gesellschaftlicher Vielfalt innerhalb und außerhalb der Polizei. Verlag für Polizeiwissenschaft, 2015. • John S. Dempsey, Linda S. Forst: An Introduction to Policing, Delmar Cengage Learning, 2015. • Runtker Rienks: Predictive Policing: Taking a Chance for a Safer Future. Korpsmedia, 2015.

	• Graham Farrell, Ken Pease: Once Bitten, Twice Bitten: Repeat Victimisation and its Implications for Crime Prevention. Crime Prevention Unit Series Paper No. 46, London, 1993.
Dozententeam:	
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung
Lerneinheitsformen: *- mode of teaching*	

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7715 Predictive Policing/Dunkelfeld	1	1	2	0	LT	M 30	1/24	5

Modulname:	**Foundations of Modern Cryptography**	*Sprache:*	*deutsch*
Modulnummer:	7716	*Abschluss:*	M.Sc.
Modulcode:	03-CFOMC	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1
Ausbildungsziele:	Vermittlung eines sehr tiefgründigen Verständnisses für die Funktionsweise und die Sicherheit asymmetrischer kryptographischer Verfahren; Vermittlung aktueller forschungsrelevanter Kenntnisse und Methoden; Vermittlung von Schlüsselqualifikationen; Schärfung von Programmierkenntnissen Conveying a very deep understanding of the operation and safety of asymmetric cryptographic methods; imparting current research-related knowledge and methods; key skills; sharpening of programming skills		
Lehrinhalte:	Computational number theory Public-key cryptosystems based on factoring and logarithms Cryptosystems based on NP-hard problems Digital signature schemes, DSS Elliptic curve cryptography Es werden wöchentlich Aufgaben gestellt, deren Lösung die Studierenden im Seminar präsentieren. Im Praktikum wird die interaktive Lernumgebung Cryptool verwendet, um die in der Vorlesung eingeführten Konzepte erfahrbar zu machen. Des Weiteren werden die in der Vorlesung vorgestellten Verfahren unter Verwendung der Programmiersprache Python und des Computeralgebrasystems Sage implementiert. In the seminar, the students present solutions to weekly exercices. The interactive learning environment Cryptool is used to experience the concepts introduced in the lecture. Furthermore, methods presented in the lecture will be implemented using the Python programming language and the computer algebra system Sage.		
Lernmethoden:	Tafelanschrieb, Beamerpräsentation, Übungsaufgaben, Rechnerpraktikum Blackboard usage, beamer presentations, exercises, computing laboratory		
Literatur:	G. Baumslag et al.: A Course in Mathematical Cryptography, De Gruyter, 2015. J. Hoffstein et al.: An Introduction to Mathematical Cryptography, SpringerVerlag, 2nd ed., 2014. ● S.D. Galbraith: Mathematics of Public Key Cryptography. Cambridge University Press, 2012. A. McAndrew: Introduction to Cryptography with Open-Source Software, CRC Press, 2011.		
Dozententeam:	Prof. Dr. rer. nat. Dohmen, Klaus (Hauptverantwortlicher) Prof. Dr. rer. nat. Tittmann, Peter		
Voraussetzungen:	keine		
Vorausges. Module:	keine		
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung		

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7716 Foundations of Modern Cryptography	2	1	1	0	LT	A	1/24	5

Modulname:	**Cryptanalysis**	*Sprache:*	*deutsch*
Modulnummer:	7717	*Abschluss:*	M.Sc.
Modulcode:	03-CCA	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2
Ausbildungsziele:	Vermittlung aktueller Kenntnisse und fortgeschrittener Methoden auf dem Gebiet der Kryptoanalyse; Befähigung zur selbstständigen Aneignung neuen Wissens; Beherrschung der internationalen Fachsprache.		
Lehrinhalte:	• Angriffsszenarien • Modelle und Aussagen zur Sicherheit kryptographischer Verfahren • Statistische Methoden der Kryptoanalyse • Lineare und differentielle Kryptoanalyse • Wörterbuchangriffe • Seitenkanalangriffe • Password-Recovery (GPU-based, CUDA) • Algebraische und zahlentheoretische Analysemethoden • Anwendungen und Fallbeispiele		
Lernmethoden:	• Tafelanschrieb • Beamerpräsentation • Rechnerpraktikum		
Literatur:	Wird in der Vorlesung bekanntgegeben.		
Dozententeam:	Prof. Dr. rer. nat. Dohmen, Klaus (Hauptverantwortlicher)		
Voraussetzungen:	Modul Foundations of Modern Cryptography		
Vorausges. Module:	keine		
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung		

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7717 Cryptanalysis	2	2	0	0	LT	A	1/24	5

Modulname:	**Digitale Werte und Güter**	*Sprache:*	*deutsch*
Modulnummer:	7718	*Abschluss:*	M.Sc.
Modulcode:	03-CDWUG	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:	Digitale Werte und Güter sind hochaktuelle Themen und haben weitreichende gesellschaftliche Einflüsse. Dank digitaler Technologien können heutzutage Transaktionen grenzenlos und ohne Einfluss von Regierungen durchgeführt werden. Dies eröffnet nicht nur große gesellschaftliche Chancen wie länderübergreifende Kommunikation oder weltweiten Geldtransfer, sondern auch Gefahren und Risiken. Unternehmen und Forschungseinrichtungen setzen in zunehmendem Maße auf Technologien wie der Blockchain, um Dienste zu dezentralisieren. Auch Regierungen haben das Thema erkannt und bemühen sich, sinnvolle Regulierungs- und Überwachungsmethoden zu implementieren. Dank des erworbenen Fach- und Methodenwissens sind die Teilnehmer in der Lage ● Dienste, die auf der Blockchaintechnologie beruhen, zu entwerfen, implementieren, administrieren und zu testen ● Unternehmen, die auf die Blockchaintechnologie setzen, zu beraten. ● Systeme, die auf der Blockchaintechnologie aufbauen, zu bewerten. Die Teilnehmer lernen und nutzen während des Studiums moderne Methoden und Werkzeuge und wenden diese für ihre eigenen Lösungen an.
Lehrinhalte:	Grundlagen ● Grundlagen Kryptografie und Kryptowährungen ● Dezentralisierung durch die Blockchain, Konsensfindung ● Erzeugen einer eigenen BTC-Adresse, Umgang mit Wallets, Erzeugen von Transaktionen, Verfolgen von Transaktionen im Netzwerk, Anonymität im Netzwerk, Alternative Mining Puzzles Erzeugen einer Altcoin ● Aufsetzen eines eigenen Altcoin-Clients ● Umsetzung einer Miningsoftware für die Altcoin ● Durchführung von Angriffsszenarien innerhalb der Altcoin Gesellschaftliche Einordnung von Bitcoin ● Regulierung ● Geschichte ● Community
Lernmethoden:	Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten ausgewählte Fälle aus dem Feld: Digitale Werte und Güter. Für das Selbststudium werden konkrete Anregungen gegeben.
Literatur:	● Andreas M. Antonopoulos: Mastering Bitcoin. O"Reilly Media, 2013. ● Melanie Swan: Blockchain: Blueprint for a New Economy. O'Reilly and Associates, 2015. ● Christof Paar, Jan Pelzl: Understaning Cryptography: A Textbook for Students and Practitioners. Springer, 2011.
Dozententeam:	Prof. Dr.-Ing. Ittner, Andreas (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7718 Digitale Werte und Güter	2	0	2	0		S 90	1/24	5

Modulname:	**Datenbankprogrammierung**	*Sprache:*	*deutsch*
Modulnummer:	7719	*Abschluss:*	M.Sc.
Modulcode:	03-CDP	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1

Ausbildungsziele:

Datenbanken haben sich als allgegenwärtiges Werkzeug im öffentlichen, wissenschaftlichen und wirtschaftlichen Leben etabliert. Diese Vorlesung soll vorhandene Kenntnisse aus einer grundlegenden Datenbankvorlesung im Bachelor vertiefen bzw. erweitern, indem insbesondere auf die Programmierung von Anwendungen im Bereich Datenbanken- und Informationssysteme eingegangen wird. Das ganze Modul soll den Bereich der Datenbankprogrammierung aus dem Fokus der Cybersecurity beleuchten. Dabei sollen Sicherheitsaspekte bei der Anwendungsentwicklung stets im Mittelpunkt stehen und der Begriff der Datenbanksicherheit mit Leben gefüllt werden.

Nach Abschluss den Moduls sind die Studierenden in der Lage sichere Anwendungen im Bereich Datenbanken- und Informationssysteme zu entwickeln und die Sicherheit von Datenbankanwendungen zu analysieren und richtig einzuschätzen.

Die Teilnehmer können nach der Vorlesung verschiedene APIs zur Anbindung von Anwenderprogrammen an Datenbanken verwenden: Schwerpunkt bildet die Programmierung mit Java und JDBC. Sie können Programme innerhalb eines Datenbanksystems erstellen, wie Stored Procedures, Trigger. Weitere Fähigkeiten stellen die Überwindung des Impedance Missmatch: Abbildung von relationalen Datentupeln auf Objekte in Java und Data Access Object Pattern dar.

Lehrinhalte:

- Bestandteile von DB-Anwendungen
- Fragestellungen bei Datenbankprogrammierung verschiedenerer Datenbank Architekturen
- Die Coddschen Regeln
- Der "Impedance Mismatch"
- Datenbankprogrammierung innerhalb der Datenbank - Stored Procedures & Trigger
- Java Database Connectivity (JDBC)
- Transaktionssteuerung
- Datenbanksicherheit
- Konsistenzkontrolle
- Datenbanksicherheit unter Verwendung von statistischen Verfahren

Lernmethoden:

In der Vorlesung werden die Prinzipien der Datenbankprogrammierung und der Datenbanksicherheit definiert und vorgestellt. Die Vorlesung erfolgt mittels Beamer-Präsentationen und Tafelanschrieb. Die Aufgaben für das Praktikum werden vorgestellt und Lösungsstrategien skizziert.

In den betreuten Praktika werden die in der Vorlesung vorgestellten Probleme der Datenbankprogrammierung und der Datenbanksicherheit von den Teilnehmern sowohl selbständig, als auch in Gruppenarbeit am Rechner implementiert. Ein Framework unterstützt diese Arbeit.

Literatur:

- Alfred Basta, Melissa Zgola: Database Security. Cengage Learning, 2011.
- David Litchfield, Chris Anley: The Database Hacker's Handbook: Defending Database Servers. John Wiley & Sons, 2005.
- George Reese: Database Programming with JDBC & Java. O"Reilly, 2000.

Dozententeam:	
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7719 Datenbankprogrammierung	2	0	2	0		S 90	1/24	5

Modulname:	**Softwarepraktikum**	*Sprache:*	*deutsch*
Modulnummer:	7720	*Abschluss:*	M.Sc.
Modulcode:	03-CSPR	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2

Ausbildungsziele:	Die Studierenden sind in der Lage, als Mitglied eines Softwareentwicklungsteams an einem realistischen Softwareprojekt von der Aufgabenstellung bis zur Inbetriebnahme des Softwaresystems zu arbeiten. Dabei werden alle Fach- und Methodenkompetenzen, die im bisherigen Masterstudium, vor allem in der Qualifizierungslinie Softwarearchitektur erworben worden sind, vom Studierenden erprobt, geübt und gefestigt. Die Studierenden können gemeinsam an einer Aufgabenstellung aus dem Bereich Cybersecurity arbeiten und übernehmen Rollenverantwortung innerhalb des Teams. Sie beherrschen ihre Kommunikationsfähigkeiten in der jeweilig festgelegten Rolle als Verantwortlicher, Fach- oder Methodenspezialist. Sie beherrschen die grundlegenden Anforderungen des Projektmanagements. Sie sind in der Lage, auf schwierige Projektsituationen so zu reagieren, dass das Gesamtziel der Erstellung eines Softwareprototypen nicht gefährdet wird. Die Studierenden sind in der Lage, professionelle und fachlich korrekte begleitende Dokumentationen zu den einzelnen Projektphasen unter Zuhilfenahme spezieller Tools zu erstellen. Sie können vollendete Projektabschnitte (Meilensteine) in einer Kurzpräsentation vor dem Entwicklungsteam, dem Dozenten-/Choachingteam und fachlich interessierten Außenstehenden so vorstellen, das die Einbettung in den Gesamtkontext immer zu erkennen ist. Die Studierenden sind für den berufliche Einsatz trainiert, softwaretechnische Prinzipien, Methoden und Werkzeuge auf praxisrelevante Fallbeispiele im Feld der Cybersecurity anzuwenden und bis zu einem Demonstrationsprototypen als Teil eines Teams zu entwickeln. Dabei können sie die ersten eigene praktischen Erfahrungen vorweisen. Sie haben Erfahrungen sowohl in klassischer als auch in agiler Vorgehensweise, da das eingesetzte und speziell dafür entwickelte Vorgehensmodell Elemente aus beiden Welten enthält.
Lehrinhalte:	• Bearbeitung einer praxisrelevanten Aufgabenstellung im Projektteam. • Bearbeitung gemäß einem Vorgehensmodell der Softwaretechnik mit agilen und klassischen Elementen, Anwendung der Lehrinhalte aus der Qualifizierungslinie Softwarearchitektur, Einsatz von zweckmäßigen UML-Werkzeugen • Projektstatusberichte und Zwischenpräsentationen gemäß Projektmeilensteine • Abschlusspräsentation der Gruppenarbeit und des Prototypen durch die Teammitglieder
Lernmethoden:	• Bildung von Projektgruppen • Visualisierungstechniken, Moderation, Präsentation, Beamereinsatz bei Teambesprechungen, • Praktisches Arbeiten am Rechner (Einsatz von CASE-Werkzeugen)
Literatur:	• Balzert, Helmut: Lehrbuch der Softwaretechnik: Entwurf, Implementierung, Installation und Betrieb, Spektrum Akademischer Verlag 2011 • Sommerville, Ian: Software Engineering - 9. Aufl., Pearson Studium 2012 • Oestereich, Bernd: Analyse und Design mit der UML 2.5: Objektorientierte Softwareentwicklung, Oldenbourg Wissenschaftsverlag 2013 • Balzert, Heide: Lehrbuch der Objektmodellierung: Analyse und Entwurf mit der U.M.L. 2, . Spektrum Akademischer Verlag 2011
Dozententeam:	Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher) Prof. Dr. rer. nat. Labudde, Dirk Prof. Dr. rer. pol. Pawlaszczyk, Dirk
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7720 Softwarepraktikum	0	0	4	0			1/24	5
	7720(T1) Teilprüfung 1						PA		
	7720(T2) Teilprüfung 2						M 20		

Modulname:	**Entwurf sicherer Systeme**	*Sprache:*	*deutsch*
Modulnummer:	7721	*Abschluss:*	M.Sc.
Modulcode:	03-CESS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:

Ziel des Moduls ist es, den Studierenden Wissen über den Entwurf sicherer Systeme zu vermitteln.

Nach dem Absolvieren dieses Kurses verfügen die Teilnehmer insbesondere über vertiefte Kenntnisse sowie Fertigkeiten bei der Planung um Umsetzung sicherer IT-Systeme.

Sie sind vertraut mit wesentlichen Design-Prinzipien und Verfahren in diesem Bereich und können das Erlernte auch praktisch anwenden.

Jeder Teilnehmer kann ein bestehendes System in Bezug auf Schwachstellen analysieren und Schutzmaßnahmen formulieren.

Lehrinhalte:

- Objektorientierte Modellierung und Entwurf, Designpattern
- Security by Design
- Defense in Depth,Multilevel Security
- Bedrohungsanalysen
- Multilateral Security
- Attack Surface Reduction
- Least Privilege
- Design for Evil
- Security through Diversity

Design und Bewertung von Security Policies, Sicherheitsmechanismen

Schwachstellen-Analyse und Angriffssimulation

Lernmethoden:

Im Rahmen der seminaristisch durchgeführten Lehrveranstaltung werden wichtige theoretische und praxisrelevante Grundlagen vermittelt. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Fallbeispielen werden Sicherheitsprobleme sowie mögliche Lösungsstrategien erörtert.

Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels Folien, Beamer-Präsentationen, Tafel dargestellt.

Literatur:

- Eckert, C.: IT-Sicherheit: Konzepte, Verfahren, Protokolle. 7. Auflage, Oldenbourg-Verlag, 2012.
- Skriha, Walter, Schmitz, Roland: Sichere Systeme: Konzepte, Architekturen und Frameworks. Springer Verlag, 2009.

Dozententeam:	Prof. Dr. rer. pol. Pawlaszczyk, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7721 Entwurf sicherer Systeme	2	0	2	0		S 90	1/24	5

Modulname:	**Datennetze/ Cloud Forensik**	*Sprache:*	*deutsch*
Modulnummer:	7722	*Abschluss:*	M.Sc.
Modulcode:	03-CDNCF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1

Ausbildungsziele:	Die Studierenden verfügen über Wissen zu den technischen Grundlagen von Cloudanwendungen. Sie sind vertraut mit den gängigen Verfahren zur Datensicherheit lokal und innerhalb der Cloud. Jeder Teilnehmer kennt die Besonderheiten und Herausforderungen bei der forensischen Analyse von Clouddaten. Alle Kursteilnehmer sind vertraut mit der Handhabung forensischer Werkzeuge, die für die Sicherstellung und Untersuchung von digitalen Spuren innerhalb der Cloud verwendet werden können und wenden diese praktisch an.
Lehrinhalte:	Cloud Computing Stack, Cloud Security and Privacy, Internet-fähige Endgeräte, Smartphones und Cloud Computing, Besonderheiten des forensischen Untersuchungsprozesses in Cloudumgebungen, technische und rechtliche Aspekte, konkrete Vorgehensmodelle und Handlungsanweisungen für die Untersuchung von Cloud-Storage-Lösungen, Verschlüsselung von Cloud-Daten, forenische Analyse aktueller Cloud-Anwendungen (Dropbox, Micosoft Aszure, Cloudflare, Amazon Cloud Front, Amazone S3, Google Drive etc.)
Lernmethoden:	Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten ausgewählte Aufgaben aus dem Bereich Datennetze / Cloud Forensik. Für das Selbststudium werden konkrete Anregungen gegeben.
Literatur:	• Raymond Choo, Darren Quick, Ben Martini : Cloud Storage Forensics. 1. Edition. Elsevier LTD, Oxford (2014) • Keyun Ruan: Cybercrime and Cloud Forensics Applications for Investigation Processes (2013) • Wilie E. May: NIST Cloud Computing 2 Forensic Science Challenges. Draft NISTIR 8006 (2014) • Josiah A. Dykstra: Digital Forensics for Infrastructure-as-a-Service Cloud Computing. Dissertation. (2013) http://www.cisa.umbc.edu/papers/dissertations/dykstra-dissertation-2013.pdf • Cloud Computing Security, Roland L. Krutz and Russel Dean Vines, 2010, Wiley.
Dozententeam:	Prof. Dr. rer. pol. Pawlaszczyk, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7722 Datennetze/ Cloud Forensik	2	0	2	0			1/24	5
7722(T1) Teilprüfung 1						PA		
7722(T2) Teilprüfung 2						M 20		

Modulname:	**Datenkompression**	*Sprache:*	*deutsch*
Modulnummer:	7723	*Abschluss:*	M.Sc.
Modulcode:	03-CDKPR	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2

Ausbildungsziele:	Das Modul vermittelt den Studierenden theoretisches und praxisorientiertes Wissen über die Algorithmen und die Verfahren der verlustfreien und verlustbehafteten Datenkompression. Der Schwerpunkt wird auf die Datenkompression von Bildern und Bildsequenzen gelegt. Nach dem Abschluss des Moduls können die Teilnehmer die Möglichkeiten und die Grenzen der Datenkompression richtig einschätzen. Sie verstehen die Herangehensweise, die Konzepte und die Techniken der Datenkompression und sind in der Lage, ausgewählte Algorithmen zur Datenkompression in Softwarekomponenten zu implementieren und sie anzuwenden.
Lehrinhalte:	Grundlagen der Datenkompression: Grundbegriffe (Redundanz, Irrelevanz), informationstheoretische Grundlagen (Entscheidungsgehalt, Entropie, Quellen- und Coderedundanz), visuelle Wahrnehmungseigenschaften des Menschen, Farbsysteme und Farbraumtransformation, Bewertungskriterien (Kompressionsverhältnis, Signalqualität); Signal- und systemtheoretische Grundlagen: Analog/Digital-Wandlung, Korrelationsfunktion, Diskrete Faltung, Transformation (Karhunen-Loéve-Transformation, Diskrete-Kosinus-Transformation, Diskrete Walsh-Hadarmard-Transformation, Diskrete-Wavelet-Transformation); Verfahren zur redundanzmindernden Codierung: Präcodierung (Lauflängen- und Phrasencodierung), Shannon-Fano-Codierung, Huffmann-Codierung, arithmetische Codierung; Methoden zur Datenreduktion: Unterabtastung, skalare Quantisierung, Vektorquantisierung, Codebuchentwurf in der Vektorquantisierung (Gradientenverfahren, Fuzzy-Sets, Methoden der statistischen Mechanik, Evolutionsstrategien); Standards der Bild- und Videocodierung (JPEG, JPEG 2000, MPEG, H.262, H.264, H.265) sowie Bildübertragungssysteme (DVB-C, DVB-S/S2, DVB-T/T2, IP-TV).
Lernmethoden:	Die Lehrinhalte werden in den Seminaren mit Hilfe von PowerPoint-Präsentationen (Notebook und Beamer) sowie Tafel und Kreide vermittelt. Unterstützt wird das Verständnis durch anschauliche Demonstrationen mithilfe von Softwaretools. Im Praktikum entwickeln die Studierenden Softwarekomponenten, mit denen sie bekannte sowie neue Algorithmen und Verfahren zur Datenkompression anwenden, ihre Wirkungsweise veranschaulichen und ihre Leistungsfähigkeit miteinander vergleichen können.
Literatur:	T. Strutz: Bilddatenkompression, Grundlagen, Codierung, Wavelets, JPEG, MPEG, H.264, 4. Aufl., Vieweg + Teubner, ISBN 978-3834804723, 2009. J.-R. Ohm, Multimedia Signal Coding and Transmission, Springer, ISBN 978-3-662-46691-9, 2015. W. Fischer, Digitale Fernseh- und Hörfunktechnik in Theorie und Praxis, 4. Aufl., Springer, ISBN 978-3642538957, 2016. R. Mäusl, Fernsehtechnik, Vom Studiosignal zum DVB-Sendesignal, 4. Aufl., Hüthig, ISBN 978-3-7785-3996-5, 2006. ● JPEG, Information technology - Digital compression and coding of continuous-tone still images - Requirements and Guidelines, T.81, 1992. ● JPEG 2000, Information technology - JPEG 2000 image coding system: Core coding system, ISO/IEC 15444-1 ... 15444-11, 2004. ● MPEG-2/H.262, Information technology, Generic coding of moving pictures and associated audio, Recommendation H.262, ISO/IEC 13818-2, 1994. ● MPEG-4AVC/H.264, Advanced video coding for generic audio-visual services, ITU-T Recommendation H.264, 2003. ● HEVC/H.265, High efficiency video coding, ITU-T Recommendation H.265, 2015. ● Electronics Letters, Journal, Institution of Engineering and Technology (IET), ISSN 0013-5194. ● IEE Proceedings - Vision, Image and Signal Processing, Journal, Institution of Engineering and Technology (IET), ISSN 1350-245X.

	• IEEE Transactions on Communications, Journal, Institute of Electrical and Electronics Engineers (IEEE), IEEE Communications Society, ISSN 0090-6778.
Dozententeam:	Prof. Dr.-Ing. Delport, Volker (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7723 Datenkompression	0	2	2	0			1/24	5
7723(T1) Teilprüfung 1						PA		
7723(T2) Teilprüfung 2						S 90		

Modulname:	**Intelligente Videoanalyse**	*Sprache:*	*deutsch*
Modulnummer:	7724	*Abschluss:*	M.Sc.
Modulcode:	03-CINVI	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:	Das Modul "Intelligente Videoanalyse" vermittelt Studierenden zunächst Grundlagen der Bilderkennung von der Aufnahme bis zur höheren Bilddeutung. Detaillierte Kenntnisse über die notwendige Beschaffenheit der zugrundeliegenden Systemarchitekturen befähigt die Studierenden infolge dazu, aufgezeigte Lösungen zu adaptieren und Videomaterialien selbständig und (halb-)automatisiert zu bearbeiten. Dies umfasst zuerst die strukturelle Analyse, bei der semantisch zusammenhängende Videosegmente identifiziert werden, wodurch sich die zu verarbeitende Datenmenge in nachfolgenden Schritten signifikant reduzieren lässt. Darauf aufbauend sollen relevante und häufig genutzte Inhalte aus diesen extrahiert und im Rahmen der IT-Forensik im Kontext der vorliegenden Szene interpretierbar gestaltet werden. Die Verarbeitung großer Mengen an audiovisuellen Aufnahmen und die gezielte Entwicklung und Optimierung von Verfahren mit hoher Genauigkeit und geringer Falsch-Alarm-Rate setzt eine flexible und nachhaltige Softwareinfrastruktur voraus. Es wird ein detailliertes Bild von der Herangehensweise, den Konzepten, Techniken und Grenzen der automatisierten Videoanalyse sowie zugehöriger Optimierungsmöglichkeiten vermittelt. Dies schließt klassische und moderne maschinelle Detektionsverfahren ein, die insbesondere den hohen qualitativen Anforderungen im Big Data-Bereich Rechnung tragen.
Lehrinhalte:	Grundlagen: • Modelle zum Bildverstehen • Entstehung, Vorverarbeitung und Analyse von Bildern • Höhere Bilddeutung Systemarchitekturen: • Struktur generischer Mustererkennungsysteme • Paradigmen und Eigenschaften holistischer Bilderkennungssysteme • Systemanforderungen, Evaluation und Optimierung • Merkmale und Klassifikation • Flexible und nachhaltige Frameworks für die Videoanalyse Strukturelle Videoanalyse: • Schnittgrenzenerkennung • Datenreduktion durch adaptive Keyframeextraktion Inhaltsbasierte Videoanalyse: • Detektion von Gesichtern, Personen, Orten und generischen Objekten • Fortgeschrittene Klassifikation mit Boosting und Deep Learning • Transferlernen aus unterschiedlichen Domänen für Big Data • 3D-Rekonstruktion und Szeneninterpretation
Lernmethoden:	Die Vorlesung vermittelt grundlegende Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel und vertieft diese in den zugehörigen Übungen und Praktika weiter, um das methodische Verständnis zu erhöhen.
Literatur:	• Burger, Wilhelm ; Burger, Mark J. (2005). Digitale Bildverarbeitung: Eine Einführung mit Java und ImageJ, Springer, 2. Auflage. • Gibbon, David C.; Liu, Zhu (2008). Introduction to Video Search Engines, Springer. • Hammoud, Riad I. (2006). Interactive Video: Algorithms and Technologies, Springer. • Ritter, Marc (2014). Optimierung von Algorithmen zur Videoanalyse : Ein Analyseframework für die Anforderungen lokaler Fernsehsender. In: Wissenschaftliche Schriftenreihe Dissertationen der Medieninformatik, Nr. 3, Universitätsverlag der Technischen Universität Chemnitz, 336 S. • Sonka, M.; Hlavac, V.; Boyle, R. (2014). Image Processing, Analysis, and Machine Vision, Cengage Learning, 2014

	• Steinmüller, Johannes (2008): Bildanalyse : Von der Bildverarbeitung zur räumlichen Interpretation von Bildern, Springer.
Dozententeam:	Prof. Dr. rer. nat. Ritter, Marc (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7724 Intelligente Videoanalyse	2	0	2	0	LT	S 60	1/24	5

Modulname:	**Cybercrime I**	*Sprache:*	*deutsch*
Modulnummer:	7701	*Abschluss:*	M.Sc.
Modulcode:	03-CCYB1	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1

Ausbildungsziele:	Straftaten im Phänomenbereich Cybercrime stellen eine wachsende Herausforderung für die Strafverfolgungsbehörden in Deutschland dar. Die bloße Anzahl solcher Straftaten nimmt jährlich zu (vgl. Bundeslagebild Cybercrime) und gleichzeitig steigt der technische Aufwand bei der Begehung solcher Straftaten ständig. Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten sowie Straftaten die mittels dieser Informationstechnik begangen werden. Im Modul Cybercrime I soll auf die sogenannte IuK-Kriminalität im engeren Sinne (Computerkriminalität) eingegangen werden. Die entsprechenden Gesetzesnormen werden vorgestellt und Begehensweisen für die einzelnen Delikte erläutert. Es wird ein besonderer Augenmerkt auf die Kriminalistik gelegt. Zu den einzelnen Begehensweisen werden Kriminalstrategie und Kriminaltaktik dargelegt. Nach Abschluss des Moduls kennen die Studierenden alle relevanten Gesetzesnormen und Begehensweisen. Sie können selbstständig effiziente Ermittlungsansätze für solche Fälle entwerfen und eigenständig aufklären. Gegen Ende des Moduls wird auf die Bedeutung der Computerkriminalität im internationalen Kontext eingegangen und internationale Normen und Verfahren dargelegt.
Lehrinhalte:	IuK Kriminalität im engeren Sinne: ● Computerbetrug (§ 263a StGB) ● Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung (§§ 269, 270 StGB) ● Datenveränderung (§ 303a) ● Computersabotage (§ 303b StGB) ● Ausspähen von Daten (§ 202a StGB) ● Abfangen von Daten (§ 202b StGB) ● Softwarepiraterie: Herstellen, Überlassen, Verbreiten oder Verschaffen von sog. "Hacker-Werkzeugen", die illegalen Zwecken dienen (§ 202c StGB) Cybercrime im Internationalen Kontext ● Die EU-Cybercrime Richtlinie ● Computer Fraud and Abuse Act und Nachfolgende Regelungen in Vereinigten Staaten ● Zwischenstaatliche Vereinbarungen, G8, UN, ITU
Lernmethoden:	Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten ausgewählte Fälle aus dem Phänomenbereich Cybercrime. Für das Selbststudium werden konkrete Anregungen gegeben.
Literatur:	● Dieter Kochheim: Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik. C.H.Beck, 2015 ● Michael Büchel, Peter Hirsch: Internetkriminalität: Phänomene-Ermittlungshilfen-Prävention (Grundlagen der Kriminalistik, Band 48). Kriminalistik, 2014. ● BKA, Cybercrime: Bundeslagebild (jährlich neu) ● Chuck Easttom, Jeff Taylor: Computer Crime, Investigation, and the Law. Cengage Learning PTR, 2010. ● United Nations: Comprehensive Study on Cybercrime. 2013 ● ITU: Understanding cybercrime: Phenomena, challenges and legal response. 2012
Dozententeam:	Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine

Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7701 Cybercrime I	2	0	2	0		S 90	1/24	5

Modulname:	**Cybercrime II**	*Sprache:*	*deutsch*
Modulnummer:	7702	*Abschluss:*	M.Sc.
Modulcode:	03-CCYB2	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2

Ausbildungsziele:	Straftaten im Phänomenbereich Cybercrime stellen eine wachsende Herausforderung für die Strafverfolgungsbehörden in Deutschland dar. Die bloße Anzahl solcher Straftaten nimmt jährlich zu (vgl. Bundeslagebild Cybercrime) und gleichzeitig steigt der technische Aufwand bei der Begehung solcher Straftaten ständig. Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten sowie Straftaten die mittels dieser Informationstechnik begangen werden. Im Modul Cybercrime II soll auf die sogenannte IuK-Kriminalität im weiteren Sinne (Tatmittel Internet) eingegangen werden. Die entsprechenden Gesetzesnormen werden vorgestellt und Begehensweisen für die einzelnen Delikte erläutert. Es wird ein besonderer Augenmerkt auf die Kriminalistik gelegt. Zu den einzelnen Begehensweisen werden Kriminalstrategie und Kriminaltaktik dargelegt. Nach Abschluss des Moduls kennen die Studierenden relevante Gesetzesnormen und Begehensweisen. Sie können selbstständig effiziente Ermittlungsansätze für solche Fälle entwerfen und eigenständig aufklären.
Lehrinhalte:	IuK Kriminalität im weiteren Sinne: ● Verbreitung pornographischer Schriften (Kinderpornographie) über das Internet ● Verbreitung von Gewaltdarstellungen im Internet ● Onlinemarktplätze (Drogenhandel, Waffenhandel, Menschenhandel) ● Urheberrechtsdelikte Cybercrime im Staatsschutz ● Internetdelikte PMK Rechts ● Internetdelikte PMK Links ● Internetdelikte PMK Islamismus Einsatz von IuK in der Organisierten Kriminalität ● Geldwäsche im Internet ● Bedeutung von IuK für grenzüberschreitende Kriminalität ● Fälschungen IuK im Strafverfahren ● IuK als falsche Beweise
Lernmethoden:	Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten ausgewählte Fälle aus dem Phänomenbereich Cybercrime. Für das Selbststudium werden konkrete Anregungen gegeben.
Literatur:	● Gerrit Manssen, Jörg Fritzsche, Robert Uerpmann-Wittzack: Strafrechtliche Verantwortlichkeit der Informationsvermittler im Netz. LIT, 2006 ● Philip Jenkins: Beyond Tolerance: Child Pornography. NYU Press, 2001. ● Jörg Kinzig: Die rechtliche Bewältigung von Erscheinungsformen der Organisierten Kriminalität, Berlin, 2004. ● Sean S. Costigan, Jake Perry: Cyberspaces and Global Affairs. Routledge, 2012. ● Bösche, Andreas: Rechtsextremismus im Internet. Schattenseiten des www. Hall 2001 ● Rüdiger Quedenfeld, Udo Mühlroth, Martin Plischke, Marc Studer: Handbuch Bekämpfung der Geldwäsche und Wirtschaftskriminalität. ESV, 2013.
Dozententeam:	Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7702 Cybercrime II	2	0	2	0		S 90	1/24	5

Modulname:	**Social Engineering und OSINT**	*Sprache:*	*deutsch*
Modulnummer:	7703	*Abschluss:*	M.Sc.
Modulcode:	03-CSEO	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:	Die Studierenden verfügen über Wissen zu den Grundlagen von Social Engineering. Sie sind mit gängigen Techniken vertraut und kennen die psychologischen Grundlagen der einzelnen Angriffsmuster. Sie kennen Abwehrstrategien gegen Social Engineering und sind in der Lage Sicherheitsrichtlinien und Schulungen zu entwickeln. Jeder Teilnehmer kennt die Möglichkeiten von OSINT (Open Source Intelligence) zur Datengewinnung. ER kann selbstständig Werkzeuge einsetzen um Daten automatisiert zu sammeln, zusammenzuführen und auszuwerten. Dabei wird er mit den Besonderheiten von Big Data konfrontiert. Alle Kursteilnehmer sind vertraut der Daten Gewinnung aus Sozialen Netzwerken, Webseiten, Medien und anderen offenen Quellen. Sie lernen Personen zu identifizieren und zu lokalisieren.
Lehrinhalte:	Grundlagen des Social Engineering • Reziprozität • Konsistenz • Commitement Andrere Techniken • Phishing • Dumpster Diving Abwehrstrategien gegen Social Engineering Grundlagen von OSINT • Arten von offenen Quellen • Automatisiertes Sammeln von Informationen • Zusammenführen von Informationen • Auswertung offener Quellen • Big Data
Lernmethoden:	Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten an ausgewählte Problemen aus dem Bereich Social Engineering und OSINT. Diese werden vertiefend diskutiert und typisch Strategien und Angriffsmuster an Beispielszenarien aufgezeigt. Für das Selbststudium werden konkrete Anregungen gegeben.
Literatur:	• Kevin D. Mitnick, William L. Simon: Die Kunst der Täuschung. Risikofaktor Mensch. mitp, Heidelberg 2006 • Cialdini, R. B.: Die Psychologie des Überzeugens. Verlag Hans Huber, 2007. • Stefan Schumacher: Psychologische Grundlagen des Social Engineering. In: Die Datenschleuder. 94, 2010 • Arthuer S. Hulnick: 'The Dilemma of Open Source Intelligence: Is OSINT Really Intelligence?', pages 229-241, The Oxford Handbook of National Security Intelligence, 2010 -Andreas Weyert : Hacking mit Kali. Francis, 2014.
Dozententeam:	Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher) M.Sc. Spranger, Michael
Voraussetzungen:	keine
Vorausges. Module:	keine

Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7703 Social Engineering und OSINT	1	0	3	0	LT	M 30	1/24	5

Modulname:	**Grundlagen der Mobilfunkforensik**	*Sprache:*	*deutsch*
Modulnummer:	7704	*Abschluss:*	M.Sc.
Modulcode:	03-CGDMF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1

Ausbildungsziele:	Weltweit existieren über 6 Mrd. Mobilfunknutzer, dies macht mehr als 90% der Weltbevölkerung aus. Bereits im Jahr 2013 waren in 85% aller Kriminalfälle mobile Endgeräte involviert. Trotz der stetig wachsenden Bedeutung mobiler Endgeräte wie Mobiltelefonen, Smart-Phones, PDAs und Musikgeräten gilt die forensische Untersuchung solcher Geräte als teuer und kompliziert. Im Modul "Grundlagen der Mobilfunkforensik" sollen verbreitete Mobilfunkstandards, Betriebssysteme und Grundlagen der Architektur von mobilen Endgeräten strukturiert dargestellt werden. In einem zweiten Teil sollen forensische Tools für mobile Endgeräte vorgestellt und Szenarien erörtert werden. Nach Abschluss des Moduls sollen die Studierenden Kompetenzen im Bereich Mobilfunkforensik der Art erworben haben, dass sie selbstständig in der Lage sind derart gelagerte Spurenträger zu untersuchen.
Lehrinhalte:	• Mobilfunksysteme: Mobilfunksysteme und Mobilfunkstandards der 2. bis 4. Generation (GSM, GPRS, UMTS, LTE), Frequenzbereiche und Frequenzregulierung, Grundlagen zellularer Mobilfunksysteme, Systemeigenschaften (Sendeleistungen, Datenraten, Übertragungsbandbreiten, usw.), Netzwerkarchitekturen und Systemkomponenten, Adressen und Kennziffern zum Auffinden eines Teilnehmers, Luftschnittstelle (Medienzugriffs- und Übertragungsverfahren, Kanalstrukturen), Mobilitätsmanagement, IT-Sicherheit. Mobilfunkforensik: • Grundlagen und Begriffe der Mobilfunkforensik • Smartcards: insbesondere SIM • Mobile Betriebssysteme: insbesondere Android, iOS, WindowsPhone • Architektur von Mobilfunkendgeräten: insbesondere Speichertechnologien • Forensische Tools: insbesondere UFED, XRY • Der IMSICatcher
Lernmethoden:	Im Rahmen des Masterstudiums werden Vorlesungen mittels Beamer-Präsentationen und Tafel gehalten, in denen wichtige theoretische und praxisrelevante Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Fallbeispielen werden Herangehensweisen an definierte Mobilfunkendgeräte sowie mögliche Lösungsstrategien erörtert. Im Praktikum werden ausgewählte Aufgabenstellungen am Spurenträger praktisch verwirklicht. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt.
Literatur:	• Satish Bommisetty, Rohit Tamma, Heather Mahalik: Practical Mobile Forensics. Packt Publishing 2014. • Wolfgang Rankl, Wolfgang Effing: Handbuch der Chipkarten: Aufbau - Funktionsweise - Einsatz von Smart Cards. 5. Auflage, Hanser, 2008. • Bernhard Walke: Mobilfunknetze und ihre Protokolle 1, Stuttgart 2001, ISBN 3-519-26430-7. • Jonathan Zdziarski : iOS Forensic Investigative Methods, 2012. M. Sauter, Grundkurs Mobile Kommunikationssysteme, Springer, 6. Aufl., 2015, ISBN-13: 978-3658083427. C. F. Lüders, Mobilfunksysteme, Vogel, 2001, ISBN-10: 3802318471. J. Hoy, Forensic Radio Survey Techniques for Cell Site Analysis, John Wiley & Sons, 2015, ISBN 9781118925737.
Dozententeam:	Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher) Prof. Dr.-Ing. Delport, Volker
Voraussetzungen:	keine
Vorausges. Module:	keine

Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7704 Grundlagen der Mobilfunkforensik	2	1	1	0		S 90	1/24	5

Modulname:	**Navigationsgeräte und Geoinformationssysteme**	*Sprache:*	*deutsch*
Modulnummer:	7705	*Abschluss:*	M.Sc.
Modulcode:	03-CNGGS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2

Ausbildungsziele:	Navigationsgeräte sind heutzutage in nahezu jedem Haushalt zu finden. Mit Hilfe dieser technischen Systeme erfolgt eine Positionsbestimmung und durch Verwendung von Geoinformationen wie Topologie-, Straßen-, Luft- oder Seekarten dementsprechend die Berechnung der zielführenden Fahrtrouten. Im Modul "Navigationsgeräte und Geoinformationssysteme" sollen die Navigationsstandards, einzelne Systeme und Grundlagen der Geoinformatik strukturiert dargestellt sowie Fundamente der geographischen Informationssysteme näher gebracht werden.
Lehrinhalte:	• Geodäsie und Kartographie, • Satellitennavigation, • Spatial Data, • Implementierung und Nutzung von Geoinformationssystemen
Lernmethoden:	Im Rahmen des Moduls finden Vorlesungen und Seminare statt. In den Vorlesungen werden die Prinzipien und Grundlagen von Navigationsgeräte und Geoinformationssystemen definiert und vorgestellt. Es werden wichtige theoretische und praxisrelevante Inhalte vermittelt sowie ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Die Vorlesung erfolgt mittels Beamer-Präsentationen und Tafelanschrieb. Die Vertiefung der Kenntnisse und Lehrinhalte erfolgt im Seminar. Anhand konkreter Fallbeispiele werden Herangehensweisen an definierte Geoinformationssysteme sowie ausgewählte Navigationsgeräte erörtert.
Literatur:	• Kahl W.: Navigation für Expeditionen, Touren, Törns und Reisen: Orientierung in der Wildnis, Schettler, 1991 • R Kothuri, A Godfrind, E Beinat: Pro oracle spatial for oracle database 11g, Dreamtech Press, 2008 • Linke W.: Orientierung mit Karte, Kompaß, GPS, Delius Klasing, 2008 • Longley P., et al.: Geographic Information System and Science, UNIGIS Amsterdam, 2001 • Schönfeld R.: Das GPS Handbuch. GPS-Handgeräte in der Praxis: Grundlagen, Basis-Funktionen, Navigation und Orientierung, Karten, Band 1 und 2, Monsenstein und Vannerdat, 2008 • Umland H.: A Short Guide to Celestial Navigation, 1997
Dozententeam:	Prof. Dr. rer. biol. hum. Stübner, Rudolf (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7705 Navigationsgeräte und Geoinformationssysteme	2	2	0	0		PA	1/24	5

Modulname:	**Komplexpraktikum Forensische Methoden**	*Sprache:*	*deutsch*
Modulnummer:	7706	*Abschluss:*	M.Sc.
Modulcode:	03-CKPFM	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:

Die Studierenden lernen in selbstgewählten Modulen praktische Verfahrensweisen aus dem Bereich Cybercrime / Cybersecurity kennen. In den einzelenen Praktika sollen die Studierenden erlernen Ihre im Studium erworbenen Fähigkeiten einzusetzen und selbst gewählte Spezialgebiete vertiefen.

Lehrinhalte:

Auswahl bis zu 2 Praktika aus:

- Forensische Digitalfotographie
- Sicherheitsmerkmale bei Wertzeichen und Urkunden
- Open Source Intelligence
- Malware Forensics
- Digitale Audioanalyse
- Methoden der Digitalen Tatortrekonstruktion
- Car Forensics
- Digitale Fallanalyse
- Digital Video Analysis
- Mobilfunkforensik

(Die Module werden entsprechend der Fortschritte der IT-Forensik aktualisiert.)

Lernmethoden:

Die Komplexpraktika finden an der Hochschule Mittweida statt. Hier sollen die theoretische Grundlagen der Studierenden zu Anwendung kommen. In diesem Zusammenhang werden ausgewählte Probleme vertiefend in Vorlesungen und Seminaren diskutiert und Strategien zur Problemlösung vorgestellt. Dann sollen die Studierenden konkrete Problemen in Kleingruppen praktisch lösen.

Literatur:

Die Literaturempfehlungen richten sich nach den gewählten Einzelpraktika im Rahmen des Komplexpraktikums.

Dozententeam:

Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher)
Prof. Dr. rer. nat. Labudde, Dirk (Hauptverantwortlicher)

Voraussetzungen:

keine

Vorausges. Module:

keine

Arbeitslast: *- workload*

150 Stunden, davon
60 Stunden Lehrveranstaltungen
90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7706 Komplexpraktikum Forensische Methoden	0	2	2	0			1/24	5
7706(T1) Teilprüfung 1						LB		
7706(T2) Teilprüfung 2						LB		

Modulname:	**Internet of Things**	*Sprache:*	*deutsch*
Modulnummer:	7707	*Abschluss:*	M.Sc.
Modulcode:	03-CIOT	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1

Ausbildungsziele:	Vermittlung von Kenntnissen über die Vernetzung und die Bestandteile des Internets der Dinge - Internet of Things. Ausgehend von einzelnen Komponenten wie RFID-Systeme, Sensoren, Aktoren, Embedded Systeme wird die vernetzte Kommunikation über das Internet demonstriert. Die Studierenden erwerben Wissen bezüglich des Aufbaus, der Funktionsweise und der Implementierung von IoT Anwendungen in Hard- und Software.
Lehrinhalte:	• Einführung in das Internets der Dinge (IoT) • Protokolle und Technologien • Sensoren, Aktoren und deren Funktionsprinzip und Anschluss • RFID-Systeme in Hard- und Software • Mikrocontroller und TCP/IP Stack als Kommunikationsendpunkte • Datenkommunikation über das Internet mit embedded Systemen und angeschlossenen Sensoren und Aktoren • Wireless Sensor Network Technologie-Funksensoren IEEE 802.15.4
Lernmethoden:	• Vorlesungen, Beamer-Präsentationen, Tafel; • Übungen und Praktika im Computerpool, Präsentation
Literatur:	• Tanenbaum, A.: Computernetzwerke, International Edition 2011 • Meyer, Martin: Kommunikationstechnik:, Vieweg +Teubner Verlag GmbH, 2011 ISBN 978-3-8348-1338-1 • Tietze, U.; Schenk, Ch.: Halbleiter-Schaltungstechnik. - Springer Verlag: Berlin Heidelberg New York u.a. - ISBN 3-540-56184-6 • www.Keil.com - uVison4/5 und 32 Bit ARM-Controller LPC1768 Dokumentation, 2014
Dozententeam:	Prof. Dr. Dr.-Ing. Luge, Hartmut (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 75 Stunden Lehrveranstaltungen 75 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7707 Internet of Things	2	2	1	0		A	1/24	5

Modulname:	**Embedded Systems Forensics und Speichertechnologien**	*Sprache:*	*deutsch*
Modulnummer:	7708	*Abschluss:*	M.Sc.
Modulcode:	03-CESFS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2

Ausbildungsziele:

Klassische PCs verschwinden zunehmend als Gerät und werden durch "intelligente Gegenstände" ersetzt. Immer kleinere embedded Systems übernehmen Aufgaben, ohne dass ihre Existenz in jedem Fall überhaupt bekannt wird. So werden miniaturisierte Computer, zum Beispiel als sogenannte Wearables, mit unterschiedlichen Sensoren direkt in Kleidungsstücke eingearbeitet. Auch der klassische Magnetspeicher verschwindet zunehmend und wird durch elektronische Flash Speicher ersetzt. Diese Entwicklung stellt ganz neue Herausforderungen an die IT-Forensik und wird zu bedeutenden Umwälzungen führen.

Im Teil "Embedded Systems Forensics" sollen verbreitete Technologien und Standards, Betriebssysteme und Grundlagen der Architektur von eingebetteten Systemen strukturiert dargestellt werden. Im Praktikum sollen Embeddeds eigenständig programmiert und ausgewertet werden. Im zweiten Teil "Speichertechnologien" sollen die Grundlagen moderner Speichertechnologien vermittelt werden. Es werden forensischen Tools für die Auswertung von eingebetteten Systemen vorgestellt und Szenarien erörtert.

Nach Abschluss des Moduls sollen die Studierenden Kompetenzen im Bereich Embbeded Systems der Art erworben haben, dass sie selbstständig in der Lage sind derart gelagerte Spurenträger zu untersuchen.

Lehrinhalte:

- Grundlagen und Begriffe eingebetteter Systeme
- typische Realisierungen - Mikrocontroller und FPGA (Grundaufbau, mbed-Standard, Beispiele)
- Programmiermethoden und Beobachtbarkeit (JTAG, Busanalysator, ...)
- RFID
- Flash-Technologien: NAND-Flash, NOR-Flash, EMMCs
- AT-Befehle bei Speichermedien

Lernmethoden:

Die Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im Seminar werden ausgewählte Probleme eingehender diskutiert. Im betreuten Praktikum bearbeiten die Studenten ausgewählte Probleme aus dem Bereich Embedded Systems Forensics und Speichertechnologien. Für das Selbststudium werden konkrete Anregungen gegeben. Anhand von konkreten Fallbeispielen werden Herangehensweisen an definierte Embeddeds sowie mögliche Lösungsstrategien erörtert.

Literatur:

- John Catsoulis: Designing Embedded Hardware. O'Reilly, 2005.
- Paolo Pavan, Roberto Bez, Piero Olivo, Enrico Zanoni: Flash Memory Cells - An Overview. IEEE 1997
- Klaus Finkenzeller: RFID Handbuch.Hanser 2008
- Niklaus Wirth: Digital Circuit Design An Introduction Textbook. Springer, 1995
- IEEE STd 1149.1 (JTAG) Testability Primer, Texas Instruments, 1997

Dozententeam:

Voraussetzungen: keine

Vorausges. Module: keine

Arbeitslast: *- workload*

150 Stunden, davon
60 Stunden Lehrveranstaltungen
90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7708 Embedded Systems Forensics und Speichertechnologien	2	1	1	0		B	1/24	5

Modulname:	**Car Forensics**	*Sprache:*	*deutsch*
Modulnummer:	7709	*Abschluss:*	M.Sc.
Modulcode:	03-CCF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:	Die Digitalisierung von Kraftfahrzeugen schreitet stetig voran. Neben elektronischen Steuergeräten, die in modernen Fahrzeugen verbaut sind, entstehen in Themenfeldern wie Car2Car-, Car2Infrastructure und Car2Person-Kommunikation neue Felder, die eine Spezialisierung der elektronischen Forensik in den Bereich Car Forensics unabdingbar machen. Trotz der stetig wachsenden Bedeutung von Kfz für die Kriminalistik die forensische Untersuchung von Fahrzeugen als teuer und kompliziert. Im Modul "Car Forensics" sollen verbreitete Standards, Bussysteme und Grundlagen der Architektur von Steuergeräten in Kfz strukturiert dargestellt werden. In einem zweiten Teil sollen forensische Tools für Fahrzeuge vorgestellt und Szenarien erörtert werden. Nach Abschluss des Moduls sollen die Studierenden Kompetenzen im Bereich Car Forensics der Art erworben haben, dass sie selbstständig in der Lage sind derart gelagerte Spurenträger zu untersuchen.
Lehrinhalte:	• Bussysteme: CAN, LIN, K-Line • Grundlagen und Begriffe der Car Forensics • Steuergeräte: insbesondere Funktion von Wegfahrsperren • Kfz-Untersuchungen • Architektur von Kfz, insbesondere Fahrzeugelektronik • Forensische Tools • Car2Car-, Car2Infrastructure und Car2Person-Kommunikation
Lernmethoden:	Das Seminar vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel in kleinen Gruppen. An Beispielen sollen die Studierenden mit der Materie vertraut gemacht werden. Im betreuten Praktikum sollen die Studenten eigenständig Datensicherungen an Kraftfahrzeugen durchführen und die gewonnenen Daten selbstständig auswerten. Im Seminar werden ausgewählte Themen vertieft und Aufgaben gemeinsam erarbeitet. Für das Selbststudium werden konkrete Anregungen gegeben.
Literatur:	In dem jungen Forschungsfeld haben sich noch keine Standardwerke etabliert. Die Studierenden erhalten Skripte und aktuelle Forschungsergebnisse im Seminar. • Thomas Käfer: Car-Forensics. Books on Demand, 2015.
Dozententeam:	Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7709 Car Forensics	0	2	2	0	PA	M 30	1/24	5

Modulname:	**IT-Governance**	*Sprache:*	*deutsch*
Modulnummer:	7710	*Abschluss:*	M.Sc.
Modulcode:	03-CITGO	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1

Ausbildungsziele:	Ziel ist es, die Studenten nach erfolgreichem Abschluss dieses Moduls zu befähigen, Führungsverantwortung zu vermitteln und Organisationseinheiten mit Informatikschwerpunkt zu übernehmen. ● Sie verstehen die Zusammenhänge von Organisation und IT-Systemen als Teil der strategischen Unternehmensplanung und -organisation, ● Die Studenten sind in der Lage IT-Systeme als Werkzeug für das Erreichen der Unternehmensziele zu verwenden, ● Sie gewinnen an Erfahrung in Planung und Organisation der Informationsver-arbeitung, ● Das erworbene Wissen kann zu Unternehmensführung unter Berücksichtigung von Erfolgsfaktoren wie z.B. Qualität, Nachhaltigkeit, Unternehmenserfolg dienen.
Lehrinhalte:	● Unternehmensziele und kritische Erfolgsfaktorendes IT-Managements zu erkennen um umzusetzen. ● Erkennen von Wettbwerbsvorteilen und damit Kernkompetenzen und Kernprozes-sen und Ermittlung der entsprechenden Schlüsselinformationen, ● Planung und Aufbau einer IT-Infrastruktur, Entscheidungskriterien und -prozesse, Entwicklungsmodelle ● IT-Controlling, Kosten-/ Nutzenanalyse, Portfoliomanagement ● Organistionoptionen für das Informationsmanagement, ZB. Eigenentwicklung, Stanardsoftware, In- und Outsourcing, Cloud, Software as a Service ● Qualitätsmanagement nach aktuellen Standards, z.B. CMM, Total Quality Management, ISO-Standards
Lernmethoden:	Vorlesung und Seminar
Literatur:	● Balzert, H.: Lehrbuch der Software- Technik 1/2. mit 3 CD-ROMs. Band 1, Band 2 Software- Entwicklung / Software-Management, Software- Qualitätssiche-rung, Unternehmensmodellierung; Spektrum-Verlag, ● Berg, Björn et al.: Hybride Softwareentwicklung Das Beste aus klassischen und agilen Methoden in einem Modell vereint; Springer, Heidelberg, 2014 ● BSI (Bundesamt für Sicherheit in der Informationstechnik): IT-Grundschutz ● Buchanan, David A.; Huczynski, Andrzej A.: Organizational Behaviour, 7th ed., Pearson Education, Harlow, UK; 2012. ● Burghardt, M.: Projektmanagement - Leitfaden für die Planung, ● Überwachung und Steuerung von Entwicklungsprojekten; Siemens Verlag: Berlin; 2012. ● Gadatsch, A.: Masterkurs IT-Controlling; Vieweg-Verlag, Wiesbaden, ● Helmke, Stefan, Uebel, Matthias: Mangementorientiertes IT-Controlling und IT-Governance, Springer-Heidelber, 2016, DOI: 10.1007/978-3-658-07990-1. ● Krcmar, H: Informationsmanagement; Springer-Verlag, Berlin ● Schmidt, Götz: Organisation und Business Analysis - Methoden und Techniken, Verlag Götz Schmidt, Wettenberg (bzw. Auch bei der Gesellschaft für Projektma-nagement wieder zu finden) ● Schneider, Kurt: Abenteuer Softwarequalität: Grundlagen für Qualitätssicherung und Qualitätsmanagement, dpunkt-Verlag, ● Suicimezov, Natalia ; Georgescu, Mircea Radu: IT-Governance in Cloud Procedia Economics and Finance, 2014, Vol.15, pp.830-835 [Peer Reviewed Jour-nal, ● Wöhe, Günther; Döring, Urlich: Einführung in die allgemeine Betriebswirt- ● schaftslehre; Verlag Vahlen; München ● Zeitschriften:

	• BISE business & information systems engineering • European Journal of information Systems (EJIS) • Information Management (I & M) ISSN: 0378-7206) • Praxis der Wirtschaftsinformatik: http://hmd.dpunkt.de/ • Information & management • Informatik Spektrum • International journal of information management • International journal of productivity and quality management • Journal of enterprise information management • IT-Governance • Management information systems • Quality management journal
Dozententeam:	Prof. Dr. rer. pol. Schmidt, Petra (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung
Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes* *V* *S* *P* *T* *PVL* *PL* *W* *C* 7710 IT-Governance 2 2 0 0 S 90 1/24 5

Modulname:	**IT-Compliance**	*Sprache:*	*deutsch*
Modulnummer:	7711	*Abschluss:*	M.Sc.
Modulcode:	03-CITC	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2

Ausbildungsziele:	Bachelorstudium in der IT-Forensik und IT-Sicherheit und verwandten Studiengängen. Die Studenten sind nach erfolgreichem Abschluss dieses Moduls in der Lage Führungsverantwortung in Organisationseinheiten mit Informatikschwerpunkt zu übernehmen. ● Die Studenten erhalten einen Überblick über die exogenen Einflüsse auf das IT-Management. ● Das erworbene Wissen kann zur Unternehmensführung unter Berücksichtigung von Erfolgsfaktoren wie z.B. Gesetzeslage, Standards, etc dienen ● organisatorische Voraussetzung zur Gewährleistung der IT-Sicherheit ● Nachhaltigkeit, Unternehmenserfolg.
Lehrinhalte:	● Die Studenten lernen die wesentlichen Inhalte der ISO 27000 kennen. ● Sie erwerben Kenntnisse über die Etablierung effektiver Informationssicherheit. ● Anwendung von Methoden und Instrumente der IT-Prüfung, und der IT-Revision an ● Kenntniserwerb in Datenschutz und Datenschutzaudit ● Erwerb der Fähigkeit mit Interessenkonflikten wie z.B. Data Mining versus Datenschutz umzugehen. ● Studenten lernen proaktiv zu denken und zu handeln, um Verstöße gegen unternehmensbezogene Rechtsvorschriften durch angemessene Aufsichts- und Überwachungsmaßnahmen zu verhindern (vgl. etwa §30 OWiG) ● Befähigung zu einer IT Revision bei Betrugsaufdeckung durchzuführen -Erlernen von Grundzügen des Risiko-Managements
Lernmethoden:	Vorlesung und Seminar
Literatur:	● Ahn, Heinz et al.: Steuerung von IT-Compliance-Management-Systemen in Kon-zern-Strukturen, in: HMD Praxis der Wirtschaftsinformatik, 2014, Vol.51(3), p.240; DOI: 10.1365/s40702-014-0028-x. ● CoBiT ● Compliance Manager, ● Emmert, Ulrich: Europäische und nationale Regelungen, in : Datenschutz und Datensicherheit - DuD, 2016, Vol.40(1), pp.34-37. DOI: 10.1007/s11623-016-0539-4. ● Helmke, Stefan, Uebel, Matthias: Mangementorientiertes IT-Controlling und IT-Governance, Springer-Heidelber, 2016, DOI: 10.1007/978-3-658-07990-1. ● Lissen, Nina et al.: IT-Services in der Cloud und ISAE 3402 - Ein praxisorientierter Leitfaden für eine erfolgreiche Auditierung, Springer, Gabler, 2014. ● ISO17021 und ISO 19011 Leitfäden zur Auditierung bzw. Zertifizierung von Managementsystemen ● ISO 27000 IT-Sicherheit ● Boris Koppenhöfer: Grundlagen Datenschutz - Eine Information für Beschäftigte; Books on Demand, 2015. ● Krupna, Carsten: Informationspflichten nach dem Bundesdatenschutzgesetz bei einem Hackerangriffen, in: Betriebs-Berater, 2014(38), p.2250 2251 2252 2253 2254. ● OWiG (Gesetz über Ordnungswidrigkeiten):IT-Compliance: Erfolgreiches Ma-nagement regulatorischer Anforderungen, Erich-Schmidt.Verlag, 2014. ● Publikationen der Deutschen Gesellschaft für Recht in der Informatik ● Sowa, Aleksandra et al.: IT-Revision, IT-Audit und IT-Compliance, Springer, Heidelberg, 2015, ISBN: 978-3-658-02807-7 ● Zeitschriften: ● IT-Governance

Dozententeam:	Prof. Dr. rer. pol. Schmidt, Petra (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7711 IT-Compliance	2	2	0	0		S 90	1/24	5

Modulname:	**Der Sachverständige vor Gericht**	*Sprache:*	*deutsch*
Modulnummer:	7712	*Abschluss:*	M.Sc.
Modulcode:	03-CSVG	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:

IT-Forensiker wie Ermittler müssen die Ergebnisse Ihrer Arbeit in Gutachten darlegen. An solche Gutachten werden definierte formale Ansprüche gestellt. Auch müssen diese Gutachten vor Gericht vertreten werden, auch hier gibt es einen formalen Rahmen der einzuhalten ist. Neben den formalen Kriterien gibt es eine Menge ungeschriebene Gesetze einzuhalten und der Sachverständige soll auch rhetorisch überzeugen.

Das Modul "Der Sachverständige vor Gericht" soll die Anforderungen an ein Gutachten beziehungsweise an einen Sachverständigenvortrag vermitteln. Daneben sollen sprachliche und rhetorische Besonderheiten im Strafprozess dargelegt werden.

Lehrinhalte:

- Das Sachverständigengutachten
- Der Sachverständigenvortrag
- Der Sachverständige in der StPO
- Juristische Rhetorik
- Sprache und Duktus des Sachverständigenvortrags

Lernmethoden:

In der Vorlesung werden wichtige theoretische und praxisrelevante Grundlagen vermittelt. Im Seminar werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand eines konkreten Falls soll eigenständig ein Gutachten geschrieben und ein Sachverständigenvortrag vorbereitet werden. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Das Erstellte Gutachten soll in einem Sachverständigenvortrag dargestellt werden. In einem Rollenspiel wird eine Gerichtsverhandlung nachgestellt.

Literatur:

- Walter Byerlein: Praxishandbuch Sachverständigenrecht. CH.. Beck, 2000.
- Harald Krammer, Jürgen Schille, Alexeander Schmidt, Alfred Tanczos: Sachverständige und ihre Gutachten. Manz 2015
- Fritjof Haft: Juristische Rhetorik. Alber Studienbuch, 2009.

Dozententeam:

Prof. Dr. rer. nat. Hummert, Christian

Prof. Dr. rer. nat. Labudde, Dirk

Voraussetzungen: keine

Vorausges. Module: keine

Arbeitslast: *- workload*

150 Stunden, davon
60 Stunden Lehrveranstaltungen
90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7712 Der Sachverständige vor Gericht	1	3	0	0			1/24	5
7712(T1) Teilprüfung 1						B		
7712(T2) Teilprüfung 2						K 20		

Modulname:	**Stochastic Models**	*Sprache:*	*deutsch*
Modulnummer:	7713	*Abschluss:*	M.Sc.
Modulcode:	03-STMOD	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1

Ausbildungsziele:	Das Hauptziel ist die Vermittlung fundierter Kenntnisse in Bereich der Modellbildung und stochastischen Simulation sowie deren Anwendung in statistischen Methoden. Die Studierenden lernen den Umgang mit verschiedenen Klassen von stochastischen Prozessen kennen. Praxisnahe Anwendungsbeispiele werden im Praktikumsteil am Computer implementiert. Auf diese Weise soll bei den Studierenden ein tiefgehendes Verständnis für die Modellierung stochastischer Prozesse herausgebildet werden. Studierende erlernen die Fähigkeit Probleme konzeptionell zu erfassen, zu strukturieren, zu modellieren und - insbesondere mittels stochastischer Simulation - eigenständig zu lösen. The main objective is the acquirement of solid knowledge of probabilistic modeling and stochastic simulation, as we ll as their application to statistical methods. Students learn to handle various classes of stochastic processes. Practical applications will be disc ussed in detail and implemented and solved using computerized methods. Based on that, students will gain a deep understanding of modeling stochastical processes. Additionally, students will acquire the abilities to comprehend practical problems conceptually, to structure and model them, and to independently solve them, particularly using stochastic simulations.
Lehrinhalte:	Im Modul Stochastische Modelle werden diskrete und kontinuierliche stochastische Prozesse vorgestellt, insbesondere Markovketten, Martingal-Prozesse, Geburts-Todesprozesse sowie Verzweigungs- und Koaleszenzprozesse eingegangen. Es wird insbesondere auf die Simulation von stochastischen Prozessen (z.B. MCMC) eingegangen sowie deren Anwendung in statistischen Verfahren (Bayes‘sche Verfahren, Approximativ Bayes'sche Verfahren). In this module discrete and continuous stochastic processes are introduced, in particular, Markov chains, Martingal-processes, birth-death processes, branching and coalescence processes. Particular focus lies on simulation techniques of stochastic processes (e.g. MCMC) as well as on their applications in statistical procedures (Bayesian and approximate Bayesian methods).
Lernmethoden:	Klassische Vorlesung (Präsentationen, Animationen und Illustrationen enthaltend), Übungen, studentische Vorträge in Seminaren, Bearbeitung von Aufgabenstellungen mittels Computeralgebrasystemen/ Matrizen-sprachen (z.B. Mathematica, Maple, MatLab) , statistischer Software (z.B. SAS, SPSS, R) und Programmiersprachen (Phython, C++). Classic lecture (pre sentations, animations and illustrations containing), exercises, student presentations in seminars, processing of tasks using computer algebra systems/ matrices-languages (e.g. , Mathematica, maple, Matlab), statistical software (e.g. , SAS, SPSS, R) and programming languages (Phython, C++).
Literatur:	H. Bauer: Wahrscheinlichkeitstheorie. de Gruyter, 4. Auflage (1991). P. Billingsley: Probability and measure. Wiley (1986). R. Durret: Probability theory and examples . Cambridge University Press, 4. Auflage (30. August 2010). G. Pflug: Stochastische Modelle in de r Informatik. B.G. Teubner Stuttgart, 1986. I. M. Sobol: Die Monte-Carlo-Methode, Taschenbücher Nr. 41. Harri Deutsch, Frankfurt a. M., 1985.
Dozententeam:	Prof. Dr. rer. nat. habil. Schneider, Kristan (Hauptverantwortlicher)
Voraussetzungen:	keine

Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7713 Stochastic Models	2	1	1	0	T	S 120	1/24	5

Modulname:	**Computational Intelligence**	*Sprache:*	*deutsch*
Modulnummer:	7714	*Abschluss:*	M.Sc.
Modulcode:	03-CINT1	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2

Ausbildungsziele:	In der Lehrveranstaltung erwerben die Studierenden Wissen über grundlegende mathematisch-algorithmische Prinzipien im maschinellen Lernen. Schwerpunkt bilden neuronale Netze und Modelle des Hebb"schen Lernens zur Mustererkennung und Klassifikation. Im Computerpraktikum erlernen die Studierenden, einfache Algorithmen in ihrem Verhalten zu modellieren und zu untersuchen. The course provides the basic principles and algorithms in CI. Particularly, neural networks for clustering and classification as well as Hebb learning are in the main focus. Completing the course, students are able to program basic models and to study their behavior.
Lehrinhalte:	Biologische Neuronen, Perzeptron, Mehrschicht-Netzwerke, Hebb"sches Lernen, Vektorquantisierung. Maschinelles Lernen mit MATLAB: Programmierung einfacher Modelle, Konvergenz. Biological neurons, perceptrons, multi-layer perceptrons , Hebbian learning, vector quantization. Machine Learning in MATLAB: programming of machine learning models in MATLAB, analysis of convergence behavior,exemplary applications.
Lernmethoden:	Kreide und Tafel, Beamer, Vorträge, Übungsaufgaben, eigene Programmierprojekte. Chalk and blackboard, slides, homework exercises, student's presentations, programming projects.
Literatur:	C. Bishop: Pattern Recognition and Machine Learning. Springer, 2007. S. Haykin: Neural Networks. Pearson Education, 2004. R. Kruse: Computational Intelligence. Teubner, 2011. H. Ritter, T. Martinetz & K. Schult en: Neural Computation and Self-Organizing Maps. Addison-Wesley, 1992. M. Mayamoto: Fuzzy Clustering. Springer 2010.
Dozententeam:	Prof. Dr. rer. nat. habil. Villmann, Thomas (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7714 Computational Intelligence	2	1	1	0		M 30	1/24	5

Modulname:	**Predictive Policing/Dunkelfeld**	*Sprache:*	*deutsch*
Modulnummer:	7715	*Abschluss:*	M.Sc.
Modulcode:	03-CPPDF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:	In der Kriminalforschung bezeichnet das Dunkelfeld die Differenz zwischen den amtlich registrierten Straftaten, dem Hellfeld, und der vermutlich begangenen Kriminalität. Allein durch die Kriminalstatistiken kann vom Hellfeld nicht auf die tatsächliche Kriminalität geschlossen werden. Daher bedarf es der Dunkelfeldforschung, um das Dunkelfeld aufzuhellen und einen systematischen Überblick über die Kriminalitätsentwicklung zu erreichen. Predictive Policing hingegen bezeichnet die Analyse von Falldaten zur Berechnung der Wahrscheinlichkeit zukünftiger Straftaten zur Steuerung des Einsatzes von Polizeikräften Nach Abschluss des Moduls können die Studierenden die amtlichen Kriminalstatistiken lesen und verstehen. Sie kennen die aktuellen Verfahren um Aussagen über das Dunkelfeld und damit über die tatsächliche Kriminalität zu treffen. Die Studierenden erhalten ein differenziertes Bild von der Möglichkeit des Predictive Policing und Aussagekraft von Aussagen über die Vorhersage von Straftaten. Sie können mit einfachen Methoden selbstständig Modelle entwickeln. Nach Abschluss des Moduls verfügen die Studierenden über einen abgerundeten Überblick über das Fachgebiet. Sie können selbstständig Modellansätze entwerfen und eigenständig berechnen.
Lehrinhalte:	• Die Polizeiliche Kriminalstatisik • Hellfeld und Dunkelfeld • Kriminalitätsmessung • Kriminalitätsanalyse und kriminalstatistische Forschung • "Ethnic Profiling" • Re-Victimisierung • Ethische Implikationen von Predicted Policing • Rational-Choice-Theorie • Boost-Hypothese • Flag-Hypothese • Near-Repeat-Victimisation • Methoden zur Vorhersage • Modellierung von Kriminalität • Extrapolationsalgorithmen • Validierung von Kriminalitätsmodellen
Lernmethoden:	Im Rahmen der seminaristischen Vorlesung werden wichtige theoretische Grundlagen vermittelt werden. In diesem Zusammenhang werden auch ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Problemen werden die Studierenden mit Herangehensweisen konfrontiert und ausgewählte Themen werden eingehend erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Im Praktikum sollen verschiedene Algorithmen aus dem Bereich Predictive Policing/Dunkelfeld in Software implementiert werden.
Literatur:	• Uwe Dörmann, Wolfgang Heinz: Zahlen sprechen nicht für sich. Aufsätze zu Kriminalstatistik, Dunkelfeld und Sicherheitsgefühl aus drei Jahrzehnten. Luchterhand, 2004. • Thomas Feltes, Benjamin Schmidt: Policing Diversity: Über den Umgang mit gesellschaftlicher Vielfalt innerhalb und außerhalb der Polizei. Verlag für Polizeiwissenschaft, 2015. • John S. Dempsey, Linda S. Forst: An Introduction to Policing, Delmar Cengage Learning, 2015. • Runtker Rienks: Predictive Policing: Taking a Chance for a Safer Future. Korpsmedia, 2015.

	• Graham Farrell, Ken Pease: Once Bitten, Twice Bitten: Repeat Victimisation and its Implications for Crime Prevention. Crime Prevention Unit Series Paper No. 46, London, 1993.
Dozententeam:	
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7715 Predictive Policing/Dunkelfeld	1	1	2	0	LT	M 30	1/24	5

Modulname:	**Foundations of Modern Cryptography**	*Sprache:*	*deutsch*
Modulnummer:	7716	*Abschluss:*	M.Sc.
Modulcode:	03-CFOMC	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1
Ausbildungsziele:	Vermittlung eines sehr tiefgründigen Verständnisses für die Funktionsweise und die Sicherheit asymmetrischer kryptographischer Verfahren; Vermittlung aktueller forschungsrelevanter Kenntnisse und Methoden; Vermittlung von Schlüsselqualifikationen; Schärfung von Programmierkenntnissen Conveying a very deep understanding of the operation and safety of asymmetric cryptographic methods; imparting current research-related knowledge and methods; key skills; sharpening of programming skills		
Lehrinhalte:	Computational number theory Public-key cryptosystems based on factoring and logarithms Cryptosystems based on NP-hard problems Digital signature schemes, DSS Elliptic curve cryptography Es werden wöchentlich Aufgaben gestellt, deren Lösung die Studierenden im Seminar präsentieren. Im Praktikum wird die interaktive Lernumgebung Cryptool verwendet, um die in der Vorlesung eingeführten Konzepte erfahrbar zu machen. Des Weiteren werden die in der Vorlesung vorgestellten Verfahren unter Verwendung der Programmiersprache Python und des Computeralgebrasystems Sage implementiert. In the seminar, the students present solutions to weekly exercices. The interactive learning environment Cryptool is used to experience the concepts introduced in the lecture. Furthermore, methods presented in the lecture will be implemented using the Python programming language and the computer algebra system Sage.		
Lernmethoden:	Tafelanschrieb, Beamerpräsentation, Übungsaufgaben, Rechnerpraktikum Blackboard usage, beamer presentations, exercises, computing laboratory		
Literatur:	G. Baumslag et al.: A Course in Mathematical Cryptography, De Gruyter, 2015. J. Hoffstein et al.: An Introduction to Mathematical Cryptography, SpringerVerlag, 2nd ed., 2014. ● S.D. Galbraith: Mathematics of Public Key Cryptography. Cambridge University Press, 2012. A. McAndrew: Introduction to Cryptography with Open-Source Software, CRC Press, 2011.		
Dozententeam:	Prof. Dr. rer. nat. Dohmen, Klaus (Hauptverantwortlicher) Prof. Dr. rer. nat. Tittmann, Peter		
Voraussetzungen:	Fundierte Kenntnisse in Algebra, Algorithmik, Wahrscheinlichkeitstheorie, objektorientierter Programmierung aus vorangegangenen BA-Studiengang Knowledge in algebra, algorithmics, probability theory, objectoriented programming from a previous BA		
Vorausges. Module:	keine		

Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7716 Foundations of Modern Cryptography	2	1	1	0	LT	A	1/24	5

Modulname:	**Cryptanalysis**	*Sprache:*	*deutsch*
Modulnummer:	7717	*Abschluss:*	M.Sc.
Modulcode:	03-CCA	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2
Ausbildungsziele:	Vermittlung aktueller Kenntnisse und fortgeschrittener Methoden auf dem Gebiet der Kryptoanalyse; Befähigung zur selbstständigen Aneignung neuen Wissens; Beherrschung der internationalen Fachsprache.		
Lehrinhalte:	• Angriffsszenarien • Modelle und Aussagen zur Sicherheit kryptographischer Verfahren • Statistische Methoden der Kryptoanalyse • Lineare und differentielle Kryptoanalyse • Wörterbuchangriffe • Seitenkanalangriffe • Password-Recovery (GPU-based, CUDA) • Algebraische und zahlentheoretische Analysemethoden • Anwendungen und Fallbeispiele		
Lernmethoden:	• Tafelanschrieb • Beamerpräsentation • Rechnerpraktikum		
Literatur:	Wird in der Vorlesung bekanntgegeben.		
Dozententeam:	Prof. Dr. rer. nat. Dohmen, Klaus (Hauptverantwortlicher)		
Voraussetzungen:	keine		
Vorausges. Module:	keine		
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung		

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7717 Cryptanalysis	2	2	0	0	LT	A	1/24	5

Modulname:	**Digitale Werte und Güter**	*Sprache:*	*deutsch*
Modulnummer:	7718	*Abschluss:*	M.Sc.
Modulcode:	03-CDWUG	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:	Digitale Werte und Güter sind hochaktuelle Themen und haben weitreichende gesellschaftliche Einflüsse. Dank digitaler Technologien können heutzutage Transaktionen grenzenlos und ohne Einfluss von Regierungen durchgeführt werden. Dies eröffnet nicht nur große gesellschaftliche Chancen wie länderübergreifende Kommunikation oder weltweiten Geldtransfer, sondern auch Gefahren und Risiken. Unternehmen und Forschungseinrichtungen setzen in zunehmendem Maße auf Technologien wie der Blockchain, um Dienste zu dezentralisieren. Auch Regierungen haben das Thema erkannt und bemühen sich, sinnvolle Regulierungs- und Überwachungsmethoden zu implementieren. Dank des erworbenen Fach- und Methodenwissens sind die Teilnehmer in der Lage ● Dienste, die auf der Blockchaintechnologie beruhen, zu entwerfen, implementieren, administrieren und zu testen ● Unternehmen, die auf die Blockchaintechnologie setzen, zu beraten. ● Systeme, die auf der Blockchaintechnologie aufbauen, zu bewerten. Die Teilnehmer lernen und nutzen während des Studiums moderne Methoden und Werkzeuge und wenden diese für ihre eigenen Lösungen an.
Lehrinhalte:	Grundlagen ● Grundlagen Kryptografie und Kryptowährungen ● Dezentralisierung durch die Blockchain, Konsensfindung ● Erzeugen einer eigenen BTC-Adresse, Umgang mit Wallets, Erzeugen von Transaktionen, Verfolgen von Transaktionen im Netzwerk, Anonymität im Netzwerk, Alternative Mining Puzzles Erzeugen einer Altcoin ● Aufsetzen eines eigenen Altcoin-Clients ● Umsetzung einer Miningsoftware für die Altcoin ● Durchführung von Angriffsszenarien innerhalb der Altcoin Gesellschaftliche Einordnung von Bitcoin ● Regulierung ● Geschichte ● Community
Lernmethoden:	Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten ausgewählte Fälle aus dem Feld: Digitale Werte und Güter. Für das Selbststudium werden konkrete Anregungen gegeben.
Literatur:	● Andreas M. Antonopoulos: Mastering Bitcoin. O"Reilly Media, 2013. ● Melanie Swan: Blockchain: Blueprint for a New Economy. O'Reilly and Associates, 2015. ● Christof Paar, Jan Pelzl: Understaning Cryptography: A Textbook for Students and Practitioners. Springer, 2011.
Dozententeam:	Prof. Dr.-Ing. Ittner, Andreas (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: - mode of teaching	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7718 Digitale Werte und Güter	2	0	2	0		S 90	1/24	5

Modulname:	**Datenbankprogrammierung**	*Sprache:*	*deutsch*
Modulnummer:	7719	*Abschluss:*	M.Sc.
Modulcode:	03-CDP	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1

Ausbildungsziele:

Datenbanken haben sich als allgegenwärtiges Werkzeug im öffentlichen, wissenschaftlichen und wirtschaftlichen Leben etabliert. Diese Vorlesung soll vorhandene Kenntnisse aus einer grundlegenden Datenbankvorlesung im Bachelor vertiefen bzw. erweitern, indem insbesondere auf die Programmierung von Anwendungen im Bereich Datenbanken- und Informationssysteme eingegangen wird. Das ganze Modul soll den Bereich der Datenbankprogrammierung aus dem Fokus der Cybersecurity beleuchten. Dabei sollen Sicherheitsaspekte bei der Anwendungsentwicklung stets im Mittelpunkt stehen und der Begriff der Datenbanksicherheit mit Leben gefüllt werden.

Nach Abschluss den Moduls sind die Studierenden in der Lage sichere Anwendungen im Bereich Datenbanken- und Informationssysteme zu entwickeln und die Sicherheit von Datenbankanwendungen zu analysieren und richtig einzuschätzen.

Die Teilnehmer können nach der Vorlesung verschiedene APIs zur Anbindung von Anwenderprogrammen an Datenbanken verwenden: Schwerpunkt bildet die Programmierung mit Java und JDBC. Sie können Programme innerhalb eines Datenbanksystems erstellen, wie Stored Procedures, Trigger. Weitere Fähigkeiten stellen die Überwindung des Impedance Missmatch: Abbildung von relationalen Datentupeln auf Objekte in Java und Data Access Object Pattern dar.

Lehrinhalte:

- Bestandteile von DB-Anwendungen
- Fragestellungen bei Datenbankprogrammierung verschiedenerer Datenbank Architekturen
- Die Coddschen Regeln
- Der "Impedance Mismatch"
- Datenbankprogrammierung innerhalb der Datenbank - Stored Procedures & Trigger
- Java Database Connectivity (JDBC)
- Transaktionssteuerung
- Datenbanksicherheit
- Konsistenzkontrolle
- Datenbanksicherheit unter Verwendung von statistischen Verfahren

Lernmethoden:

In der Vorlesung werden die Prinzipien der Datenbankprogrammierung und der Datenbanksicherheit definiert und vorgestellt. Die Vorlesung erfolgt mittels Beamer-Präsentationen und Tafelanschrieb. Die Aufgaben für das Praktikum werden vorgestellt und Lösungsstrategien skizziert.

In den betreuten Praktika werden die in der Vorlesung vorgestellten Probleme der Datenbankprogrammierung und der Datenbanksicherheit von den Teilnehmern sowohl selbständig, als auch in Gruppenarbeit am Rechner implementiert. Ein Framework unterstützt diese Arbeit.

Literatur:

- Alfred Basta, Melissa Zgola: Database Security. Cengage Learning, 2011.
- David Litchfield, Chris Anley: The Database Hacker's Handbook: Defending Database Servers. John Wiley & Sons, 2005.
- George Reese: Database Programming with JDBC & Java. O"Reilly, 2000.

Dozententeam:	
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7719 Datenbankprogrammierung	2	0	2	0		S 90	1/24	5

Modulname:	**Softwarepraktikum**	*Sprache:*	*deutsch*
Modulnummer:	7720	*Abschluss:*	M.Sc.
Modulcode:	03-CSPR	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2

Ausbildungsziele:	Die Studierenden sind in der Lage, als Mitglied eines Softwareentwicklungsteams an einem realistischen Softwareprojekt von der Aufgabenstellung bis zur Inbetriebnahme des Softwaresystems zu arbeiten. Dabei werden alle Fach- und Methodenkompetenzen, die im bisherigen Masterstudium, vor allem in der Qualifizierungslinie Softwarearchitektur erworben worden sind, vom Studierenden erprobt, geübt und gefestigt. Die Studierenden können gemeinsam an einer Aufgabenstellung aus dem Bereich Cybersecurity arbeiten und übernehmen Rollenverantwortung innerhalb des Teams. Sie beherrschen ihre Kommunikationsfähigkeiten in der jeweilig festgelegten Rolle als Verantwortlicher, Fach- oder Methodenspezialist. Sie beherrschen die grundlegenden Anforderungen des Projektmanagements. Sie sind in der Lage, auf schwierige Projektsituationen so zu reagieren, dass das Gesamtziel der Erstellung eines Softwareprototypen nicht gefährdet wird. Die Studierenden sind in der Lage, professionelle und fachlich korrekte begleitende Dokumentationen zu den einzelnen Projektphasen unter Zuhilfenahme spezieller Tools zu erstellen. Sie können vollendete Projektabschnitte (Meilensteine) in einer Kurzpräsentation vor dem Entwicklungsteam, dem Dozenten-/Choachingteam und fachlich interessierten Außenstehenden so vorstellen, das die Einbettung in den Gesamtkontext immer zu erkennen ist. Die Studierenden sind für den berufliche Einsatz trainiert, softwaretechnische Prinzipien, Methoden und Werkzeuge auf praxisrelevante Fallbeispiele im Feld der Cybersecurity anzuwenden und bis zu einem Demonstrationsprototypen als Teil eines Teams zu entwickeln. Dabei können sie die ersten eigene praktischen Erfahrungen vorweisen. Sie haben Erfahrungen sowohl in klassischer als auch in agiler Vorgehensweise, da das eingesetzte und speziell dafür entwickelte Vorgehensmodell Elemente aus beiden Welten enthält.
Lehrinhalte:	• Bearbeitung einer praxisrelevanten Aufgabenstellung im Projektteam. • Bearbeitung gemäß einem Vorgehensmodell der Softwaretechnik mit agilen und klassischen Elementen, Anwendung der Lehrinhalte aus der Qualifizierungslinie Softwarearchitektur, Einsatz von zweckmäßigen UML-Werkzeugen • Projektstatusberichte und Zwischenpräsentationen gemäß Projektmeilensteine • Abschlusspräsentation der Gruppenarbeit und des Prototypen durch die Teammitglieder
Lernmethoden:	• Bildung von Projektgruppen • Visualisierungstechniken, Moderation, Präsentation, Beamereinsatz bei Teambesprechungen, • Praktisches Arbeiten am Rechner (Einsatz von CASE-Werkzeugen)
Literatur:	• Balzert, Helmut: Lehrbuch der Softwaretechnik: Entwurf, Implementierung, Installation und Betrieb, Spektrum Akademischer Verlag 2011 • Sommerville, Ian: Software Engineering - 9. Aufl., Pearson Studium 2012 • Oestereich, Bernd: Analyse und Design mit der UML 2.5: Objektorientierte Softwareentwicklung, Oldenbourg Wissenschaftsverlag 2013 • Balzert, Heide: Lehrbuch der Objektmodellierung: Analyse und Entwurf mit der U.M.L. 2, . Spektrum Akademischer Verlag 2011
Dozententeam:	Prof. Dr. rer. nat. Hummert, Christian (Hauptverantwortlicher) Prof. Dr. rer. nat. Labudde, Dirk Prof. Dr. rer. pol. Pawlaszczyk, Dirk
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*	*Bezeichnung des Modulelementes*	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
	7720 Softwarepraktikum	0	0	4	0			1/24	5
	7720(T1) Teilprüfung 1						S 90		
	7720(T2) Teilprüfung 2						PA		

Modulname:	**Entwurf sicherer Systeme**	*Sprache:*	*deutsch*
Modulnummer:	7721	*Abschluss:*	M.Sc.
Modulcode:	03-CESS	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:

Ziel des Moduls ist es, den Studierenden Wissen über den Entwurf sicherer Systeme zu vermitteln.

Nach dem Absolvieren dieses Kurses verfügen die Teilnehmer insbesondere über vertiefte Kenntnisse sowie Fertigkeiten bei der Planung um Umsetzung sicherer IT-Systeme.

Sie sind vertraut mit wesentlichen Design-Prinzipien und Verfahren in diesem Bereich und können das Erlernte auch praktisch anwenden.

Jeder Teilnehmer kann ein bestehendes System in Bezug auf Schwachstellen analysieren und Schutzmaßnahmen formulieren.

Lehrinhalte:

- Objektorientierte Modellierung und Entwurf, Designpattern
- Security by Design
- Defense in Depth,Multilevel Security
- Bedrohungsanalysen
- Multilateral Security
- Attack Surface Reduction
- Least Privilege
- Design for Evil
- Security through Diversity

Design und Bewertung von Security Policies, Sicherheitsmechanismen

Schwachstellen-Analyse und Angriffssimulation

Lernmethoden:

Im Rahmen der seminaristisch durchgeführten Lehrveranstaltung werden wichtige theoretische und praxisrelevante Grundlagen vermittelt. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Fallbeispielen werden Sicherheitsprobleme sowie mögliche Lösungsstrategien erörtert.

Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels Folien, Beamer-Präsentationen, Tafel dargestellt.

Literatur:

- Eckert, C.: IT-Sicherheit: Konzepte, Verfahren, Protokolle. 7. Auflage, Oldenbourg-Verlag, 2012.
- Skriha, Walter, Schmitz, Roland: Sichere Systeme: Konzepte, Architekturen und Frameworks. Springer Verlag, 2009.

Dozententeam:	Prof. Dr. rer. pol. Pawlaszczyk, Dirk (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7721 Entwurf sicherer Systeme	2	0	2	0		S 90	1/24	5

Modulname:	**Datennetze/Cloud Forensics**	*Sprache:*	*deutsch*
Modulnummer:	7722	*Abschluss:*	M.Sc.
Modulcode:	03-CDNCF	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	1

Ausbildungsziele:

Die Studierenden verfügen über Wissen zu den technischen Grundlagen von Cloudanwendungen.

Sie sind vertraut mit den gängigen Verfahren zur Datensicherheit lokal und innerhalb der Cloud.

Jeder Teilnehmer kennt die Besonderheiten und Herausforderungen bei der forensischen Analyse von Clouddaten.

Alle Kursteilnehmer sind vertraut mit der Handhabung forensischer Werkzeuge, die für die Sicherstellung und Untersuchung von digitalen Spuren innerhalb der Cloud verwendet werden können und wenden diese praktisch an.

Lehrinhalte:

Cloud Computing Stack, Cloud Security and Privacy, Internet-fähige Endgeräte, Smartphones und Cloud Computing, Besonderheiten des forensischen Untersuchungsprozesses in Cloudumgebungen, technische und rechtliche Aspekte, konkrete Vorgehensmodelle und Handlungsanweisungen für die Untersuchung von Cloud-Storage-Lösungen, Verschlüsselung von Cloud-Daten, forenische Analyse aktueller Cloud-Anwendungen (Dropbox, Micosoft Aszure, Cloudflare, Amazon Cloud Front, Amazone S3, Google Drive etc.)

Lernmethoden:

Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten ausgewählte Aufgaben aus dem Bereich Datennetze / Cloud Forensik. Für das Selbststudium werden konkrete Anregungen gegeben.

Literatur:

- Raymond Choo, Darren Quick, Ben Martini : Cloud Storage Forensics. 1. Edition. Elsevier LTD, Oxford (2014)
- Keyun Ruan: Cybercrime and Cloud Forensics Applications for Investigation Processes (2013)
- Wilie E. May: NIST Cloud Computing 2 Forensic Science Challenges. Draft NISTIR 8006 (2014)
- Josiah A. Dykstra: Digital Forensics for Infrastructure-as-a-Service Cloud Computing. Dissertation. (2013) http://www.cisa.umbc.edu/papers/dissertations/dykstra-dissertation-2013.pdf
- Cloud Computing Security, Roland L. Krutz and Russel Dean Vines, 2010, Wiley.

Dozententeam: Prof. Dr. rer. pol. Pawlaszczyk, Dirk (Hauptverantwortlicher)

Voraussetzungen: keine

Vorausges. Module: keine

Arbeitslast: *- workload*

150 Stunden, davon
60 Stunden Lehrveranstaltungen
90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7722 Datennetze/Cloud Forensics	2	0	2	0			1/24	5
7722(T1) Teilprüfung 1						S 90		
7722(T2) Teilprüfung 2						M 20		

Modulname:	**Datenkompression**	*Sprache:*	*deutsch*
Modulnummer:	7723	*Abschluss:*	M.Sc.
Modulcode:	03-CDKPR	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	2

Ausbildungsziele:	Das Modul vermittelt den Studierenden theoretisches und praxisorientiertes Wissen über die Algorithmen und die Verfahren der verlustfreien und verlustbehafteten Datenkompression. Der Schwerpunkt wird auf die Datenkompression von Bildern und Bildsequenzen gelegt. Nach dem Abschluss des Moduls können die Teilnehmer die Möglichkeiten und die Grenzen der Datenkompression richtig einschätzen. Sie verstehen die Herangehensweise, die Konzepte und die Techniken der Datenkompression und sind in der Lage, ausgewählte Algorithmen zur Datenkompression in Softwarekomponenten zu implementieren und sie anzuwenden.
Lehrinhalte:	Grundlagen der Datenkompression: Grundbegriffe (Redundanz, Irrelevanz), informationstheoretische Grundlagen (Entscheidungsgehalt, Entropie, Quellen- und Coderedundanz), visuelle Wahrnehmungseigenschaften des Menschen, Farbsysteme und Farbraumtransformation, Bewertungskriterien (Kompressionsverhältnis, Signalqualität); Signal- und systemtheoretische Grundlagen: Analog/Digital-Wandlung, Korrelationsfunktion, Diskrete Faltung, Transformation (Karhunen-Loéve-Transformation, Diskrete-Kosinus-Transformation, Diskrete Walsh-Hadarmard-Transformation, Diskrete-Wavelet-Transformation); Verfahren zur redundanzmindernden Codierung: Präcodierung (Lauflängen- und Phrasencodierung), Shannon-Fano-Codierung, Huffmann-Codierung, arithmetische Codierung; Methoden zur Datenreduktion: Unterabtastung, skalare Quantisierung, Vektorquantisierung, Codebuchentwurf in der Vektorquantisierung (Gradientenverfahren, Fuzzy-Sets, Methoden der statistischen Mechanik, Evolutionsstrategien); Standards der Bild- und Videocodierung (JPEG, JPEG 2000, MPEG, H.262, H.264, H.265) sowie Bildübertragungssysteme (DVB-C, DVB-S/S2, DVB-T/T2, IP-TV).
Lernmethoden:	Die Lehrinhalte werden in den Seminaren mit Hilfe von PowerPoint-Präsentationen (Notebook und Beamer) sowie Tafel und Kreide vermittelt. Unterstützt wird das Verständnis durch anschauliche Demonstrationen mithilfe von Softwaretools. Im Praktikum entwickeln die Studierenden Softwarekomponenten, mit denen sie bekannte sowie neue Algorithmen und Verfahren zur Datenkompression anwenden, ihre Wirkungsweise veranschaulichen und ihre Leistungsfähigkeit miteinander vergleichen können.
Literatur:	T. Strutz: Bilddatenkompression, Grundlagen, Codierung, Wavelets, JPEG, MPEG, H.264, 4. Aufl., Vieweg + Teubner, ISBN 978-3834804723, 2009. J.-R. Ohm, Multimedia Signal Coding and Transmission, Springer, ISBN 978-3-662-46691-9, 2015. W. Fischer, Digitale Fernseh- und Hörfunktechnik in Theorie und Praxis, 4. Aufl., Springer, ISBN 978-3642538957, 2016. R. Mäusl, Fernsehtechnik, Vom Studiosignal zum DVB-Sendesignal, 4. Aufl., Hüthig, ISBN 978-3-7785-3996-5, 2006. ● JPEG, Information technology - Digital compression and coding of continuous-tone still images - Requirements and Guidelines, T.81, 1992. ● JPEG 2000, Information technology - JPEG 2000 image coding system: Core coding system, ISO/IEC 15444-1 ... 15444-11, 2004. ● MPEG-2/H.262, Information technology, Generic coding of moving pictures and associated audio, Recommendation H.262, ISO/IEC 13818-2, 1994. ● MPEG-4AVC/H.264, Advanced video coding for generic audio-visual services, ITU-T Recommendation H.264, 2003. ● HEVC/H.265, High efficiency video coding, ITU-T Recommendation H.265, 2015. ● Electronics Letters, Journal, Institution of Engineering and Technology (IET), ISSN 0013-5194. ● IEE Proceedings - Vision, Image and Signal Processing, Journal, Institution of Engineering and Technology (IET), ISSN 1350-245X.

	• IEEE Transactions on Communications, Journal, Institute of Electrical and Electronics Engineers (IEEE), IEEE Communications Society, ISSN 0090-6778.
Dozententeam:	Prof. Dr.-Ing. Delport, Volker (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7723 Datenkompression	0	2	2	0			1/24	5
7723(T1) Teilprüfung 1						PA		
7723(T2) Teilprüfung 2						PA		

Modulname:	**Intelligente Videoanalyse**	*Sprache:*	*deutsch*
Modulnummer:	7724	*Abschluss:*	M.Sc.
Modulcode:	03-CINVI	*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Wahlpflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	3

Ausbildungsziele:	Das Modul "Intelligente Videoanalyse" vermittelt Studierenden zunächst Grundlagen der Bilderkennung von der Aufnahme bis zur höheren Bilddeutung. Detaillierte Kenntnisse über die notwendige Beschaffenheit der zugrundeliegenden Systemarchitekturen befähigt die Studierenden infolge dazu, aufgezeigte Lösungen zu adaptieren und Videomaterialien selbständig und (halb-)automatisiert zu bearbeiten. Dies umfasst zuerst die strukturelle Analyse, bei der semantisch zusammenhängende Videosegmente identifiziert werden, wodurch sich die zu verarbeitende Datenmenge in nachfolgenden Schritten signifikant reduzieren lässt. Darauf aufbauend sollen relevante und häufig genutzte Inhalte aus diesen extrahiert und im Rahmen der IT-Forensik im Kontext der vorliegenden Szene interpretierbar gestaltet werden. Die Verarbeitung großer Mengen an audiovisuellen Aufnahmen und die gezielte Entwicklung und Optimierung von Verfahren mit hoher Genauigkeit und geringer Falsch-Alarm-Rate setzt eine flexible und nachhaltige Softwareinfrastruktur voraus. Es wird ein detailliertes Bild von der Herangehensweise, den Konzepten, Techniken und Grenzen der automatisierten Videoanalyse sowie zugehöriger Optimierungsmöglichkeiten vermittelt. Dies schließt klassische und moderne maschinelle Detektionsverfahren ein, die insbesondere den hohen qualitativen Anforderungen im Big Data-Bereich Rechnung tragen.
Lehrinhalte:	Grundlagen: • Modelle zum Bildverstehen • Entstehung, Vorverarbeitung und Analyse von Bildern • Höhere Bilddeutung Systemarchitekturen: • Struktur generischer Mustererkennungsysteme • Paradigmen und Eigenschaften holistischer Bilderkennungssysteme • Systemanforderungen, Evaluation und Optimierung • Merkmale und Klassifikation • Flexible und nachhaltige Frameworks für die Videoanalyse Strukturelle Videoanalyse: • Schnittgrenzenerkennung • Datenreduktion durch adaptive Keyframeextraktion Inhaltsbasierte Videoanalyse: • Detektion von Gesichtern, Personen, Orten und generischen Objekten • Fortgeschrittene Klassifikation mit Boosting und Deep Learning • Transferlernen aus unterschiedlichen Domänen für Big Data • 3D-Rekonstruktion und Szeneninterpretation
Lernmethoden:	Die Vorlesung vermittelt grundlegende Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel und vertieft diese in den zugehörigen Übungen und Praktika weiter, um das methodische Verständnis zu erhöhen.
Literatur:	• Burger, Wilhelm ; Burger, Mark J. (2005). Digitale Bildverarbeitung: Eine Einführung mit Java und ImageJ, Springer, 2. Auflage. • Gibbon, David C.; Liu, Zhu (2008). Introduction to Video Search Engines, Springer. • Hammoud, Riad I. (2006). Interactive Video: Algorithms and Technologies, Springer. • Ritter, Marc (2014). Optimierung von Algorithmen zur Videoanalyse : Ein Analyseframework für die Anforderungen lokaler Fernsehsender. In: Wissenschaftliche Schriftenreihe Dissertationen der Medieninformatik, Nr. 3, Universitätsverlag der Technischen Universität Chemnitz, 336 S. • Sonka, M.; Hlavac, V.; Boyle, R. (2014). Image Processing, Analysis, and Machine Vision, Cengage Learning, 2014

	• Steinmüller, Johannes (2008): Bildanalyse : Von der Bildverarbeitung zur räumlichen Interpretation von Bildern, Springer.
Dozententeam:	Prof. Dr. rer. nat. Ritter, Marc (Hauptverantwortlicher)
Voraussetzungen:	keine
Vorausges. Module:	keine
Arbeitslast: *- workload*	150 Stunden, davon 60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7724 Intelligente Videoanalyse	2	0	2	0	LT	S 60	1/24	5

Modulname:	**Masterprojekt**	*Sprache:*	*deutsch*
Modulnummer:	7725	*Abschluss:*	M.Sc.
Modulcode:		*Häufigkeit:*	jahresweise
Pflicht/Wahl:	Pflicht	*Dauer:*	1
Studiengang:	CY-M 2017 Cybercrime/Cybersecurity	*Semester:*	4
Dozententeam:			
Voraussetzungen:	keine		
Vorausges. Module:	keine		
Arbeitslast: *- workload*	900 Stunden, davon 15 Stunden Lehrveranstaltungen 885 Stunden Vor- und Nachbereitung, Prüfungsvorbereitung		

Lerneinheitsformen: *- mode of teaching*

Bezeichnung des Modulelementes	*V*	*S*	*P*	*T*	*PVL*	*PL*	*W*	*C*
7725 Masterprojekt	0	0	0	1			6/24	30
7725(T1) Masterarbeit						MA		
7725(T2) Kolloquium						K 30		