Brandenburgische
Technische Universität
Cottbus - Senftenberg

24/2017 **Amtliches Mitteilungsblatt der BTU Cottbus–Senftenberg** **26.09.2017**

I n h a l t

Herausgeber: Brandenburgische Technische Universität Cottbus - Senftenberg, Der Präsident
Redaktion: Abteilung Lehre und Studium, Referat Qualitätsmanagement Studium und Lehre
Druck: BTU Cottbus - Senftenberg
Auflage: 15

Fachspezifische Prüfungs- und Studienordnung für den Master-Studiengang Cyber Security

vom 22. September 2017

Nach dem Brandenburgischen Hochschulgesetz (BbgHG) vom 28. April 2014 (GVBl. I/14 Nr. 18), zuletzt geändert durch das Gesetz vom 01. Juli 2015 (GVBl. I/15 Nr. 18), gemäß des § 5 Abs. 1 Satz 2, § 9 Abs. 5 Satz 2 i. V. m. §§ 19 Abs. 2 Satz 1, 22 Abs. 2 Satz 1, 72 Abs. 2 Satz 1 und § 1 der Allgemeinen Prüfungs- und Studienordnung für Master-Studiengänge an der BTU Cottbus–Senftenberg vom 12. September 2016 (AMbl. 14/2016) gibt sich die Brandenburgische Technische Universität Cottbus–Senftenberg (BTU) folgende Satzung:

Inhaltsverzeichnis

§ 1 Geltungsbereich

[1]Diese Satzung regelt die fachspezifischen Besonderheiten des Master-Studiengangs Cyber Security. [2]Sie ergänzt die Allgemeine Prüfungs- und Studienordnung (RahmenO-MA) für Master-Studiengänge der BTU vom 12. September 2016 (AMbl. 14/2016). [3]Im Zweifel haben die Allgemeinen Bestimmungen Vorrang.

§ 2 Inhaltliches Profil des Studiengangs, Ziele des Studiums

[1]Ziel des universitären Studiengangs Cyber Security ist die Vermittlung von vertieften fachlichen Kenntnissen, Fähigkeiten und Methoden auf dem Gebiet der IT-Sicherheit, die die Studierenden zum selbständigen wissenschaftlichen Arbeiten befähigt und sie an aktuelle Forschungsthemen der IT-Sicherheit heranführt. [2]Die Absolventinnen und Absolventen dieses Studiengangs sind in der Lage, IT-Systeme aus dem Blickwinkel der IT-Sicherheit zu bewerten und Lösungen zu erarbeiten, die dem aktuellen Stand der Technik unter Beachtung der organisatorischen und juristischen Randbedingungen entsprechen. [3]Der Studiengang verbindet Informatikinhalte mit einer starken ingenieurtechnischen Ausbildung in IT-Sicherheit in Theorie und Praxis. [4]Das soll die Absolventinnen und Absolventen befähigen, anspruchsvolle Aufgaben in Industrie, Verwaltung und Wissenschaft zur Umsetzung von IT-Sicherheitsstrategien zu übernehmen oder in der Forschung zur Weiterentwicklung des Fachgebiets beizutragen.

§ 3 Graduierung, Abschlussbezeichnung

Bei erfolgreichem Abschluss des Master-Studiengangs Cyber Security wird der akademische Grad „Master of Science“ (M. Sc.) verliehen.

§ 4 Spezielle Zugangs- und Immatrikulationsvoraussetzungen

(1) Die Teilnahme am Master-Studium setzt die Immatrikulation entsprechend den Rahmenbedingungen der BTU voraus.

(2) [1]Grundsätzliche Voraussetzung für die Zulassung zum Master-Studium ist ein erster berufsqualifizierender Abschluss (mind. Bachelor-Grad) in einem informatik-nahen Studiengang. [2]Insbesondere qualifiziert ein Bachelor-Abschluss in Informatik, IT-Sicherheit oder Mathematik mit Nebenfach Informatik. [3]Ausreichende inhaltliche Nähe des Abschlusses liegt vor, wenn die Ausbildung in theoretischer, praktischer, angewandter und technischer Informatik und in Mathematik einen dem Bachelor-Studiengang Informatik an der BTU vergleichbaren Umfang aufweist.

(3) [1]Die Prüfung auf ausreichende inhaltliche Nähe eines Abschlusses führt der Prüfungsausschuss durch. [2]In Fällen einer bedingten

Gleichwertigkeit kann der Ausschuss das Nachholen von Modulen festlegen.

(4) [1]Cyber Security ist ein internationaler Studiengang. [2]Die Lehr- und Prüfungssprache ist Englisch. [3]Für die Zulassung zum Studiengang ist von allen Studienbewerberinnen und Studienbewerbern daher der Nachweis ausreichender Sprachkenntnisse gemäß § 3 Abs. 3 der Immatrikulationsordnung der BTU vom 13. Juli 2015 (AMbl. 01/2015) zu erbringen.

§ 5 Regelstudienzeit, Studienumfang

(1) [1]Die Regelstudienzeit des Master-Studiums umfasst vier Semester. [2]Der Umfang des Master-Studiums beträgt 120 Leistungspunkte (LP) nach dem ECTS (European Credit Transfer System).

(2) [1]Das Studium beginnt im Wintersemester. [2]Der Studiengang wird als Vollzeitstudium angeboten.

§ 6 Studienaufbau und Studiengestaltung

(1) [1]Das Master-Studium gliedert sich in vier Semester mit jeweils 30 LP. [2]Die Struktur des Studiums ist durch das Curriculum (Anlage 1) festgelegt. [3]Das Curriculum gliedert sich in einen Grundlagenbereich und einen Vertiefungsbereich sowie in ein fachübergreifendes Studium, ein Industriepraktikum und die Master-Arbeit.

(2) Der Grundlagenbereich „Cyber Security Basics“ umfasst 22 LP und besteht aus den in Anlage 2 angegebenen Pflichtmodulen.

(3) [1]Der Vertiefungsbereich umfasst 54 LP und gliedert sich in zwei Wahlpflichtbereiche (siehe Anlage 2) und das Studienprojekt. [2]Aus dem Wahlpflichtbereich „Cyber Security Methods“ sind Module im Umfang von mindestens 28 LP und aus dem Wahlpflichtbereich „Computer Science“ Module im Umfang von mindestens 12 LP zu erbringen.

(4) Das zweimonatige Industriepraktikum sollte in der vorlesungsfreien Zeit durchgeführt werden.

§ 7 Besondere Regelungen zur Prüfungsorganisation

Es bestehen keine besonderen Regelungen zur Prüfungsorganisation.

§ 8 Master-Arbeit

(1) [1]Die Master-Arbeit wird in Englisch verfasst und i. d. R. im vierten Semester durchgeführt. [2]Sie wird mit 30 LP bewertet. [3]Die Bearbeitungsdauer der schriftlichen Arbeit beträgt fünf Monate. [4]Die Anmeldung zur Master-Arbeit kann erst erfolgen, wenn alle Module einschließlich des Studienprojekts im Umfang von 82 LP erfolgreich abgeschlossen sind. [5]Das Industriepraktikum kann auch nach Abschluss der Master-Arbeit absolviert werden.

(2) [1]Das Thema der Master-Arbeit muss zwingend einen Bezug zur Thematik Cyber Security (IT Sicherheit) haben. [2]Dies ist bei der Anmeldung durch den Prüfungsausschuss zu bestätigen.

§ 9 Weitere ergänzende Regelungen

Es bestehen keine weiteren ergänzenden Regelungen.

§ 10 Inkrafttreten, Außerkrafttreten, Übergangsregelungen

(1) [1]Diese Satzung tritt am Tag nach ihrer Bekanntmachung in Kraft.

(2) Diese Prüfungs- und Studienordnung tritt nach Ablauf von vier Semestern nach der festgesetzten Regelstudienzeit des Studiengangs und der letztmaligen Immatrikulation außer Kraft.

Ausgefertigt auf Grund der Beschlüsse des Fakultätsrats der Fakultät 1 MINT - Mathematik, Informatik, Physik, Elektro- und Informationstechnik vom 12. Oktober 2016 sowie 12. Juli 2017, der Stellungnahme des Senats vom 15. Dezember 2016, der Genehmigung durch den Präsidenten der Brandenburgischen Technischen Universität Cottbus–Senftenberg vom 07. März 2017 sowie der Genehmigung durch das Ministerium für Wissenschaft, Forschung und Kultur des Landes Brandenburg vom 30. Mai 2017.

Cottbus, den 22. September 2017

Prof. Dr.-Ing. Dr. h.c. (NUWM, UA) DSc. h.c.
Jörg Steinbach
Hon.-Prof. (ECUST, CN)
Präsident

Anlage 1: Übersicht der Module, Status, Leistungspunkte (LP)

Modulbereiche/Module	Status	Bewertung	Leistungspunkte
Grundlagenmodule			**22**
Cyber Security Basics	P	Prüfung	22
Vertiefungsmodule			**54**
Cyber Security Methods	WP	Prüfung*	28-34
Computer Science	WP	Prüfung*	12-18
Study Project	P	Studienleistung	8
			44
Fachübergreifendes Studium	WP	Prüfung	6
Internship	P	Studienleistung	8
Master Thesis	P	Prüfung	30
Summe			**120**

P = Pflicht, WP = Wahlpflicht
*) Seminare und Praktika, die mit einer Studienleistung abschließen, können im Umfang von maximal 12 LP als Vertiefungsmodule angerechnet werden.

Anlage 2: Module des Grundlagen- und Vertiefungsbereichs

Modultitel	Leistungspunkte
Cyber Security Basics (Pflichtmodule)	
Introduction into Cyber Security	8
Cryptography	8
IT Security Law	6
Cyber Security Methods (Wahlpflichtmodule)	
Cryptographic Protocols	6
Pervasive System Security	6
Security of Resource-constraint Systems	6
Software Security	6
Hands on Knowledge for Side Channel Attacks	6
Cyber Security Application Areas	6
Cyber Security Lab	6
Seminar	4
Computer Science (Wahlpflichtmodule)	
Introduction to Web Services and eBusiness Technologies	6
Web-Technologies Lab	4
Dependability and Fault Tolerance	6
Foundations of Data Mining	6
Neural Networks and Learning Theory	8
Software Project Management	8
Internet - Functionality, Protocols, Applications	8
Wireless Sensor Networks: Concepts, Protocols and Applications	6
Introduction into Concurrency	8
Software Dependability	8
Software Testing	8
Operating Systems II (Multi-Level Memory Management)	6
Distributed and Parallel Systems II (Concurrency, Replication and Consistency)	6

Die Studiengangsleitung kann auf Antrag die Liste der wählbaren Module ergänzen.

Anlage 3: Regelstudienplan

Module	**Leistungspunkte (LP) im Semester**				**Summe LP**
	1	**2**	**3**	**4**	
Grundlagenmodule Cyber Security Basics (Pflicht)					
Introduction into Cyber Security	8				8
Cryptography		8			8
IT Security Law			6		6
Summe Grundlagenmodule	**8**	**8**	**6**		**22**
Vertiefungsmodule					
Wahlpflichtmodule Cyber Security Methods	16	10	8		34
Wahlpflichtmodule Computer Science	6	6			12
Study Project			8		8
Summe Vertiefungsmodule	**22**	**16**	**16**		**54**
Fachübergreifendes Studium		6			6
Internship			8		8
Master Thesis				30	30
Summe		**6**	**8**	**30**	**44**
Summe Studium	**30**	**30**	**30**	**30**	**120**

Anlage 4: Praktikumsordnung für das Berufspraktikum

1. Gültigkeit

Diese Ordnung gilt für das Berufspraktikum des Master-Studiengangs Cyber Security der Brandenburgischen Technischen Universität Cottbus–Senftenberg in Verbindung mit der gültigen Prüfungs- und Studienordnung.

2. Zweck des Praktikums

Das Berufspraktikum ist darauf angelegt, im Studium erworbenes Fach- und Methodenwissen in der Praxis anzuwenden und umzusetzen. Dies schließt insbesondere die Arbeit im Team ein. Das Praktikum dient darüber hinaus der Rückkopplung zwischen industrieller Praxis einerseits und Forschung und Lehre andererseits. Die Suche nach geeigneten Praktikumsplätzen ist Aufgabe der Studierenden. Lehrstühle können und sollen Hilfe bei der Vermittlung leisten, um diese Rückkopplung zu ermöglichen.

3. Anmeldung

Das Praktikum ist spätestens vier Wochen vor Antritt von der Mentorin oder vom Mentor zu genehmigen. Die Genehmigung umfasst das Thema, das aufnehmende Unternehmen und die Betreuerin bzw. den Betreuer im Unternehmen.

4. Praktikum im Ausland

Die Durchführung von Praktika im Ausland wird ausdrücklich begrüßt. Sie unterliegen jedoch denselben Richtlinien wie Praktika im Inland. Hingewiesen wird auf Austauschprogramme und Vermittlungen des Deutschen Akademischen Austauschdienstes (DAAD).

5. Praktikumsbetriebe

Zu den potenziell geeigneten Unternehmen gehören Firmen, die auf dem Gebiet der IT-Sicherheit tätig sind, aber auch hochschulunabhängige Forschungseinrichtungen (z. B. Institute der Fraunhofer-Gesellschaft). In Ausnahmefällen können Praktika an Hochschuleinrichtungen (z. B. Rechenzentren) genehmigt werden. Die Praktikantin oder der Praktikant soll durch eine fest angestellte Mitarbeiterin oder einen fest angestellten Mitarbeiter betreut werden, die oder der über einen Diplom- oder Master-Abschluss verfügt. Diese Ansprechpartnerin oder dieser Ansprechpartner muss im Bericht genannt werden und als Ansprechpartnerin bzw. Ansprechpartner zur Verfügung stehen. Sie oder er soll die Arbeit der oder des Studierenden anleiten und für Fragen und Vorschläge ansprechbar sein.

6. Betreuung

Die Betreuung auf Seiten der Hochschule ist Aufgabe der Mentorin oder des Mentors. Wissenschaftliche Mitarbeiterinnen oder Mitarbeiter können an der Betreuung mitwirken. Erwünscht und vorgesehen sind regelmäßige Konsultationen zwischen der Mentorin oder dem Mentor und der industriellen Betreuerin oder dem entsprechenden industriellen Betreuer.

7. Dauer und Aufteilung des Praktikums

Das Praktikum hat eine Dauer von mindestens zwei Monaten. Es soll nach Möglichkeit in einem Stück absolviert werden. Eine Praktikumswoche entspricht der Wochenarbeitszeit des jeweiligen Unternehmens. Der Urlaubsanspruch wird durch das Bundesurlaubsgesetz geregelt. Längere durch Krankheit ausgefallene Arbeitszeit muss nachgeholt werden, bei kürzerer Ausfallzeit entscheidet der Prüfungsausschuss. Es wird empfohlen, während des Praktikums eine Zeitplanung vorzunehmen sowie ein Tagebuch zu führen

8. Praktikumsbericht

Über die gesamte Dauer des Praktikums ist ein Bericht zu erstellen (Umfang ca. 3.500 bis 4.000 Wörter) und der industriellen Betreuerin bzw. dem industriellen Betreuer vorzulegen. Dieser Bericht muss den üblichen Anforderungen an wissenschaftliche Abhandlungen genügen. Der Bericht kann nach Absprache mit der Mentorin oder dem Mentor auch in englischer Sprache erstellt werden. Er soll beschreiben:

- den Praktikumsbetrieb,
- das Tätigkeitsfeld des Betriebes bzw. der Abteilung,
- Aufgabenstellung, Stand der Technik,
- Vorgehensweise, Lösung,
- Reflexion der eigenen Tätigkeit, Erfahrungen, Erkenntnisgewinn, Anwendbarkeit von Kenntnissen / Fähigkeiten aus dem Studium.

Der Bericht ist von der industriellen Betreuerin bzw. vom industriellen Betreuer abzuzeichnen. Der Bericht ist spätestens acht Wochen nach Beendigung der Tätigkeit der Mentorin bzw. dem Mentor vorzulegen.