Ordnung des Studiengangs Master of Science (M.Sc.) IT-Sicherheit

Ausführungsbestimmungen
mit Anhängen
I: Studien- und Prüfungsplan
II: Kompetenzbeschreibungen
III: Modulhandbuch (*nur elektronisch veröffentlicht*)
vom 18.07.2014

TECHNISCHE UNIVERSITÄT DARMSTADT

Beschluss des Fachbereichsrats am 18.07.2014

In Kraft-Treten der Ordnung am 01.10.2015

Aufgrund der Genehmigung des Präsidiums der TU Darmstadt vom 19.03.2015 (Az.: 652-7-1) wird die Ordnung des Studiengangs Master of Science (M.Sc.) IT-Sicherheit des Fachbereichs Informatik vom 18.07.2014 gemäß den Allgemeinen Prüfungsbestimmungen der Technischen Universität Darmstadt (APB) bekannt gemacht.

Darmstadt, 19.03.2015

Der Präsident der TU Darmstadt
Prof. Dr. Hans Jürgen Prömel

0. Inhaltsverzeichnis der Ordnung

1. Ausführungsbestimmungen

zu § 2 (1): Akademische Grade

Der Studiengang Master of Science (M.Sc.) „IT-Sicherheit“ wird vom Fachbereich Informatik der Technischen Universität Darmstadt getragen. Die Technische Universität Darmstadt verleiht nach Erreichen der im Studiengang erforderlichen Summe von 120 Kreditpunkten den akademischen Grad Master of Science (M.Sc.).

zu § 3 (5): Zeitpunkt der Prüfungen

Die Zeitpunkte der Prüfungen (Fachprüfungen und Studienleistungen) sind in Anhang I dieser Ausführungsbestimmungen, dem Studien und Prüfungsplan, festgelegt.

zu §5 (4), (5): Module, Bestandteile und Art der Prüfung

In Anhang I dieser Ausführungsbestimmungen, dem Studien- und Prüfungsplan, und in Anhang III, dem Modulhandbuch, ist die Art der Prüfungsleistungen (mündlich, schriftlich, Sonderform, Hausarbeit, etc.) festgelegt.

zu § 11 (4): Allgemeine Zulassungsvoraussetzungen - Sprachkenntnisse

Unterrichtssprache des Studiengangs ist deutsch. Einzelne Lehrveranstaltungen werden aber auch in englischer Sprache angeboten.

zu § 17a: Zugangsvoraussetzungen zu Masterstudiengängen

1. Zugangsvoraussetzung zum Masterstudiengang ist ein Bachelorabschluss in der Fachrichtung „Informatik“ an der TU Darmstadt (Referenzstudiengang) oder ein Studiengang, der wesentlich gleiche Kompetenzen vermittelt (vergleichbarer Studiengang). Die relevanten Kompetenzen sind in Anhang II dieser Ausführungsbestimmungen, den Kompetenzbeschreibungen, benannt. Diese Voraussetzungen werden im Rahmen einer Eingangsprüfung überprüft.

2. Die Eingangsprüfung besteht aus der formellen Prüfung der im Rahmen der Immatrikulation vorzulegenden schriftlichen Unterlagen und erforderlichenfalls aus der materiellen Prüfung.

3. Ergibt sich aus der formellen Prüfung der schriftlichen Unterlagen ein Defizit an Kompetenzen, dessen Aufarbeitung Leistungen im Umfang von mehr als 30 CP erforderlich machen, erfolgt keine Zulassung zum Studiengang. Der Antragsteller ist über die fehlenden Kompetenzen und die zum Erwerb der fehlenden Kompetenzen abzuleistenden Module zu unterrichten.

4. Ergeben sich bei der Prüfung der schriftlichen Unterlagen Zweifel am Vorliegen der erforderlichen Kompetenzen, werden diese im Rahmen der weiteren materiellen Eingangsprüfung überprüft. Diese Überprüfung erfolgt durch eine schriftliche Prüfung von 90 min Dauer oder durch eine mündliche Prüfung von 20-30 min Dauer. Die Prüfungskommission legt Form und Zeitpunkt der materiellen Eingangsprüfung fest und benennt einen Prüfer oder eine Prüferin. Der Prüfer oder die Prüferin bestimmt Form und Inhalt der Prüfung mit dem Ziel, die Eignung der Studienbewerberin oder des Studienbewerbers für den Studiengang Master of Science (M.Sc.) IT Sicherheit an der Technischen Universität Darmstadt festzustellen. Die Eingangsprüfung wird unter Beteiligung einer Beisitzerin oder eines Beisitzers durchgeführt.

5. Der Prüfer oder die Prüferin entscheidet auf der Grundlage der Eingangsprüfung, ob der Bewerber oder die Bewerberin die i.S.d. Nr. 4 erforderlichen Kompetenzen besitzt und stellt nach § 17a Abs. 4 APB fest, ob die Bewerberin oder der Bewerber den für das Masterstudium erforderlichen Kenntnisstand besitzt, oder ob sie oder er gegebenenfalls unter Auflagen zuzulassen oder eine Zulassung wegen mangelnden Kenntnisstandes abzulehnen ist. Die Eingangsprüfung kann im gleichen Bewilligungszeitraum nicht wiederholt werden.

6. Die Zulassung kann mit Auflagen verbunden werden, die den Bewerber bzw. die Bewerberin in die Lage versetzen sollen, fehlende Kenntnisse aus dem Bachelorstudium nachzuweisen oder in einer

festgelegten Zeit während des Masterstudiums an der TU Darmstadt nachzuholen. Die Auflagen müssen im Zulassungsbescheid aufgeführt sein und innerhalb von zwei Semestern erfüllt werden. Auflagen können auf zwei Arten erfüllt werden: 1. Der Bewerber weist die dadurch geforderten Kompetenzen durch bereits in einem Hochschulstudium erbrachte Leistungen nach. 2. Der Bewerber weist nach, dass er die geforderten Kompetenzen besitzt, indem er Fachprüfungen in den Auflagen erfolgreich ablegt. Werden die Auflagen nicht in der festgelegten Zeit erfüllt, wird die Immatrikulation in den Master-Studiengang widerrufen.

7. Die Eingangsprüfung ist keine selbständige Prüfungsentscheidung, sondern unselbständiger Teil der Zulassungsentscheidung.

zu § 18 (1): Zugangsvoraussetzungen

Die empfohlenen Zugangsvoraussetzungen zu Modulen sind in Anhang III zu diesen Ausführungsbestimmungen, dem Modulhandbuch, im Abschnitt „Voraussetzungen zur Teilnahme“ in der Modulbeschreibung eines Moduls festgelegt.

zu § 22 (2), (3): Durchführung der Prüfungen

Die Dauer der schriftlichen und der mündlichen Prüfungen ist im Studien- und Prüfungsplan (Anhang I) und dem Modulhandbuch (Anhang III) festgelegt.

zu § 23 (5): Abschlussarbeit - Bearbeitungszeit

Die Abschlussarbeit muss innerhalb von 26 Wochen angefertigt und eingereicht werden. Sie hat einen Arbeitsaufwand von 900 Stunden.

zu §25 (3): Bildung und Gewichtung von Noten

In Anhang III, den Modulbeschreibungen, ist jeweils festgelegt, mit welchem Gewicht die Noten der Fachprüfungen und Studienleistungen in das Gewicht der Modulnote eingehen. Soweit nichts anderes festgelegt ist, gehen die Noten der Prüfungsleistungen der Modulteile entsprechend der den Leistungen zugeordneten Kreditpunkte ein.

Die Abschlussarbeit wird mit einem universitätsöffentlichen Kolloquium abgeschlossen. Die Bewertung des universitätsöffentlichen Kolloquiums erfolgt durch den Prüfer oder die Prüferin und geht zu 15% in die Bewertung der Master-Thesis ein.

zu §27 (5): Bestehen und Nichtbestehen - Wahlbereiche

Die in Wahlbereichen abzulegenden Prüfungsleistungen sind in Anhang I dieser Ausführungsbestimmungen, dem Studien- und Prüfungsplan, festgelegt.

zu §28 (3): Gesamtnote

In Anhang I dieser Ausführungsbestimmungen, dem Studien- und Prüfungsplan, ist festgelegt, mit welchem Gewicht die Modulnote in die Endnote eingehen. Soweit in Anhang I nicht anders festgelegt, gehen die Modulnoten entsprechend der in den Modulen erworbenen Kreditpunkte in die Gesamtnote ein.

zu §30 (1), (2): Wiederholung der Prüfung

Auf Antrag kann ein Wahlmodul einmalig aus wichtigem Grund gewechselt werden. In diesem Fall entfallen die nach §30 Abs. 1 Satz 1 erforderlichen Wiederholungsprüfungen. Der Wechsel bedarf der Zustimmung der Prüfungskommission. Eine Ablehnung muss schriftlich begründet werden.

zu §31 (1): Zweite Wiederholung

Bei schriftlichen Prüfungen kann die zweite Wiederholungsprüfung im Einvernehmen von Prüfenden und Prüflingen auch mündlich erfolgen.

zu §35 (1): Prüfungszeugnis

Im Zeugnis der bestandenen Masterprüfung werden neben den Prüfungen mit Angaben der Modulnoten die jeweils erworbenen Kreditpunkte aufgeführt.

zu §39 (2): In-Kraft-Treten

Diese Ausführungsbestimmungen treten am 1. Oktober 2015 in Kraft. Sie werden in der Satzungsbeilage der Technischen Universität Darmstadt veröffentlicht. Mit In-Kraft-Treten dieser Ausführungsbestimmungen treten die Ausführungsbestimmungen vom 08.07.2011 (Satzungsbeilage 5.11s) außer Kraft. Bereits begonnene Studiengänge können auf Antrag nach den bisherigen Ausführungsbestimmungen zu Ende geführt werden, der Antrag ist innerhalb eines Jahres nach In-Kraft-Treten dieser Ausführungsbestimmungen beim zuständigen Studienbüro zu stellen.

Anhang I	Studien- und Prüfungsplan
Anhang II	Kompetenzbeschreibungen
Anhang III	Modulhandbuch

Darmstadt, den 24.02.2015

Der Dekan des Fachbereichs Informatik
der Technischen Universität Darmstadt

1.1. Anhang I: Studien- und Prüfungsplan

Masterstudiengang
M.Sc. IT-Sicherheit

TECHNISCHE UNIVERSITÄT DARMSTADT

Studien- und Prüfungsplan (Anhang I)

Legende	
Bewertungssystem:	St = Standard (benotet); bnb = bestanden/nicht bestanden
Prüfungsform:	s = schriftlich; m = mündlich; SF = Sonderform; H=Hausarbeit; f = fakultativ (schriftlich 60-120 min/mündlich i.d.R. 30 min), R = Referat, …
Dauer:	Dauer der Prüfung in min (optional)
Gewichtung:	Bei Kursen = Gewichtung der Prüfungsnote für die Modulnote Bei Modulen = Gewichtung der Modulnote für die Gesamtnote
SWS:	Semesterwochenstunden
Status:	o = obligatorisch (=Pflichtprüfung)
Art der Lehrform:	VL=Vorlesung; PS=Proseminar; S=Seminar; Ü=Übung; iV=integrierte Lehrveranstaltung; VÜ=Vorlesung mit Übung; tt=Tutorium; PL=Praktikum in der Lehre; Pr=Praktikum; Pp=Projektpraktikum; Pj=Projekt; Ku=Kurs
CP:	Kreditpunkte

		Prüfungsleistungen					Kurs				Semester			
											Die Zuordnung der Prüfungen zu Semestern hat empfehlenden Charakter.			
		Fachprüfung	Studienleistung	Prüfungsform	Dauer (min)	Gewichtung	SWS	Status	Lehrform	gesamt	Arbeitsaufwand pro Semester (CP)			
TUCaN-Nr. und Zuordnung von CP zu Modulbausteinen haben informativen Charakter. Die Anrechnung der CPs erfolgt nach Abschluss des Moduls.										CP	1.	2.	3.	4.
Pflichtbereich							**12**			**18**				
20-00-0085	Einführung in die Kryptographie	St		f				o						
20-00-0085-iv	Einführung in die Kryptographie						4		iV			6		
20-00-0219	IT Sicherheit	St		f				o						
20-00-0219-iv	IT Sicherheit						4		iV			6		
20-00-0581	Embedded System Security	St		f				o						
20-00-0581-iv	Embedded System Security						4		iV			6		
Wahlbereich Cryptography **Vorlesungen und Übungen oder integrierte Lehrveranstaltungen, die genannten Lehrveranstaltungen sind Beispiele aus den jeweiligen Katalogen.** **Prüfungsform und -dauer nach Vorgabe des anbietenden Fachbereichs.**										**6-42**				
20-00-0063	Public Key Infrastrukturen	St		f				f						
20-00-0063-iv	Public Key Infrastrukturen						4		iV			6		
20-00-0585	Kryptoplexität	St		f				f						
20-00-0585-iv	Kryptoplexität						4		iV			6		
…	…													
…	…													
Wahlbereich System Security **Vorlesungen und Übungen oder integrierte Lehrveranstaltungen, die genannten Lehrveranstaltungen sind Beispiele aus den jeweiligen Katalogen.** **Prüfungsform und -dauer nach Vorgabe des anbietenden Fachbereichs.**										**6-42**				
20-00-0512	Netzsicherheit	St		f				f						
20-00-0512-iv	Netzsicherheit						4		iV			6		
20-00-0561	Secure, Trusted and Trustworthy Computing	St		f				f						
20-00-0561-iv	Secure, Trusted and Trustworthy Computing						4		iV			6		
…	…													
…	…													
Wahlbereich Software Security **Vorlesungen und Übungen oder integrierte Lehrveranstaltungen, die genannten Lehrveranstaltungen sind Beispiele aus den jeweiligen Katalogen.** **Prüfungsform und -dauer nach Vorgabe des anbietenden Fachbereichs.**										**6-42**				
20-00-0599	Privacy Enhancing Technologies	St		f				f						
20-00-0599-iv	Privacy Enhancing Technologies						2		iV			3		
20-00-0362	Formale Methoden der Informationssicherheit	St		f				f						
20-00-0362-iv	Formale Methoden der Informationssicherheit						4		iV			6		
…	…													
…	…													
Wahlbereich Selected Complementary Topics **Vorlesungen und Übungen oder integrierte Lehrveranstaltungen, die genannten Lehrveranstaltungen sind Beispiele aus den jeweiligen Katalogen.** **Prüfungsform und -dauer nach Vorgabe des anbietenden Fachbereichs.**										**6-42**				
20-00-0748	Mobile Netze	St		f				f						
20-00-0748-iv	Mobile Netze						4		iV			6		
20-00-0341	Software Engineering - Design and Construction	St		f				f						
20-00-0341-iv	Software Engineering - Design and Construction						4		iV			6		
…	…													
…	…													
Wahlbereich Studienbegleitende Leistungen **Auswahl von Lehrveranstaltungen aus dem Katalog des MSc IT-Sicherheit der Seminare (mindest. 1, max. 2), dem Katalog des MSc IT-Sicherheit der Praktika in der Lehre (max. 1) und dem Katalog des MSc IT-Sicherheit der Praktika, Projektpraktika und ähnlicher Veranstaltungen (mindest. 1).** **Prüfungsform und -dauer nach Vorgabe des anbietenden Fachbereichs.**										**12-15**				
20-00-0646	Security and Privacy in Information Technology		St	SF				f						
20-00-0646-se	Security and Privacy in Information Technology						2		S			3		
20-00-0615	Smartphone Security		St	SF				f						

20-00-0615-pr	Smartphone Security						4		Pr		6			
…	…													
…	…													
Master Thesis (Die schriftliche Arbeit geht mit 85% und das Kolloquium mit 15% in die Note für die Master Thesis ein.)		SF		s						**30**				
20-AM-5000	Master Thesis	St		TH		85%		o	X					30
		St		m		15%								
Summe										**120**	120			

* Sollte eines der Pflichtfächer bereits im Bachelorstudiengang absolviert worden sein, können die entsprechenden CP stattdessen in den Wahlpflichtbereichen erbracht werden.

1.2. Anhang II: Kompetenzbeschreibungen

1.2.1. Eingangskompetenzen

1.2.1.1. Für den Master of Science Studiengang IT-Sicherheit erforderliche Kompetenzen

Die folgenden sind nicht die einzigen Kompetenzen, die im Bachelor of Science Studiengang Informatik der TU Darmstadt erworben werden. Sie sind aber charakteristisch für den Anspruch des Studiengangs und auch wesentliche Voraussetzungen für die Fortsetzung des Studiums in einem der darauf aufbauenden Masterstudiengänge. Jeder Absolvent dieses Studiengangs hat – neben dem Erwerb anderer Kompetenzen – folgende Erfahrungen gesammelt:

1. Absolventen sind intensiv und umfassend geübt in der weitgehend selbstständigen Bearbeitung von Aufgabenstellungen auf allen Inhalten der Pflichtveranstaltungen des Studiengangs. Dabei bedeutet

- *intensiv und umfassend*, dass diese Erfahrungen nicht nur punktuell gesammelt werden (etwa in eigens dafür eingerichteten Lehrveranstaltungen), sondern dass sich dies durch das gesamte Studium hindurch zieht, wenn auch nicht unbedingt in jeder Lehrveranstaltung in gleichem Maße.

- *selbstständig*, dass die Beratungsangebote im Wesentlichen der Aufgabenklärung und ersten Einstiegshilfe dienen, darüber hinaus die Studierenden die Aufgabe – je nach Vorgabe – einzeln oder im Team aber selbstständig bearbeiten müssen.

  Die Aufgabenstellungen sind häufig Transferaufgaben und erfordern Kreativität und Abstraktion bei der Lösung. Das Niveau lässt sich wie folgt genauer beschreiben:

  - *Mathematik*: die Fähigkeit, typische Beweise aus einem beweisorientierten Mathematikstudium zu verstehen und in zur Vorlesung analogen elementaren Fällen auch selbst korrekt zu führen. Die entsprechenden Kompetenzen werden u.a. in den Veranstaltungen *Mathematik 1, 2, 3 für Informatiker* erworben.

  - *Theoretische Informatik:* die Fähigkeit, mathematische Notationen und Methoden zur Fundierung von Konzepten der Informatik einzusetzen insbesondere zur formalen Modellierung und Verifikation von Soft- und Hardwaresystemen. Veranstaltungen, in denen diese Kompetenzen erworben werden, sind u.a. *Aussagen- und Prädikatenlogik; Automaten, formale Sprachen und Entscheidbarkeit; Formale Methoden im Softwareentwurf; Modellierung, Spezifikation und Semantik*.

  - *Praktische Informatik*: die Fähigkeit,

    - selbständig aus einer Problembeschreibung die zur Lösung erforderlichen Standardalgorithmen und Datenstrukturen entsprechend den funktionalen und nicht-funktionalen Anforderungen auszuwählen bzw. unter Zugrundelegung von bekannten Strategien neue Algorithmen und Datenstrukturen zur Problemlösung zu konstruieren und einzuschätzen ggf. unter Berücksichtigung von Parallelität.

- die einzelnen Bestandteile einer Programmiersprache, die in den Vorlesungen nacheinander separat eingeführt werden, selbstständig und ohne analoges Beispiel im Rahmen einer Programmieraufgabe zu einer Gesamtlösung zusammenzuführen.
- Programmieraufgaben in unterschiedlichen, auch parallelen, Programmiersprachen zu lösen, die verschiedenen Paradigmen folgen, unterschiedliche Anwendungsbereiche haben und auf der ganzen Bandbreite an Abstraktionsebenen angesiedelt sind.
- Die Qualität der erstellten Implementierungen durch formalisierte Testverfahren und Entwurfsmethoden sicherzustellen
- diese Kenntnisse in praktisch relevanten Bereichen der Informatik wie Netzwerken und verteilten Systemen, Visual Computing, Informationsmanagement und Computational Engineering/Robotik, sowie der Erstellung von Programmierwerkzeugen selber anzuwenden. Dabei sollen jeweils auch nicht-funktionale Aspekte, insbesondere auch die Sicherheit der erstellten IT-Systeme, berücksichtigt werden.

Diese Kompetenzen werden u.a. erworben in den Veranstaltungen *Funktionale und objektorientierte Programmierkonzepte; Algorithmen und Datenstrukturen; Einführung in den Compilerbau; Systemnahe und parallele Programmierung; Bachelorpraktikum; Informationsmanagement; Computational Engineering und Robotik; Computer-Netzwerke und verteilte Systeme; Computersystemsicherheit; Software Engineering; Visual Computing.*

- *Technische Informatik*: die Fähigkeit,
  - die einzelnen Entwurfsprinzipien und Grundelemente von digitalen Schaltungen, wie sie in den Vorlesungen nacheinander separat eingeführt werden, selbstständig und ohne analoges Beispiel im Rahmen einer Hardware-Entwurfsaufgabe zu einer Gesamtlösung zusammenzuführen.
  - Entwurfsaufgaben auf unterschiedlichen Abstraktionsebenen und aus unterschiedlichen Anwendungsbereichen durch strukturierte Entwurfsmethoden in verschiedenen Beschreibungssprachen und unter Einsatz eines Spektrums von Entwurfswerkzeugen zu lösen und bezüglich geeigneter Gütemaße zu evaluieren
  - die Interaktion von Computer-, Prozessor- und Mikroarchitekturen zu verstehen und daraus für die System- und Anwendungssoftwareebene passende Implementierungsentscheidungen zu treffen.

  Veranstaltungen, in denen diese Kompetenzen erworben werden, sind u. a. *Digitaltechnik; Rechnerorganisation; Betriebssysteme; Architekturen und Entwurf von Rechnersystemen.*

2. Absolventen sind durch die Organisation des Studiums geübt in der selbstständigen Arbeitsorganisation unter engen Rahmenbedingungen auf verschiedenen Zeitskalen (bis hin zu einem Umfang von mehreren Semestern).

1.2.1.2. Kriterien der Eingangsprüfung zum Master of Science Studiengang IT-Sicherheit

Alle oben beschriebenen Erfahrungen sind wesentlich für die erfolgreiche Absolvierung der Master of Science Studiengänge; *Distributed Software Systems*; *Informatik*; *Internet- und Web-basierte Systeme*; *IT-Sicherheit* und. Insbesondere wesentlich ist, dass diese Erfahrungen im Zusammenhang mit den Inhalten der Grundlagenveranstaltungen gesammelt werden insbesondere in den Kernfächern der Informatik (gegliedert in grundlegende und vertiefende Pflichtveranstaltungen), auf denen der gewählte Masterstudiengang beruht.

Im Folgenden werden die Anforderungen detailliert definiert, die uneingeschränkt notwendig sind, um den Master of Science Studiengang *IT-Sicherheit* erfolgreich zu absolvieren:

1. Es müssen die oben definierten Erfahrungen für die Kernfächer der Informatik nachgewiesen sein. Konkret müssen Inhalte aus folgenden Veranstaltungen im Umfang von mindestens 60 CP abgedeckt sein:
    a. Inhalte der grundlegenden Pflichtveranstaltungen: *Funktionale und objektorientierte Programmierkonzepte; Algorithmen und Datenstrukturen; Digitaltechnik; Rechnerorganisation; Systemnahe und parallele Programmierung; Betriebssysteme; Einführung in den Compilerbau; Automaten, Formale Sprachen und Entscheidbarkeit; Aussagen- und Prädikatenlogik; Formale Methoden im Software-Entwurf* und
    b. Inhalte der vertiefende Pflichtveranstaltungen: *Architekturen und Entwurf von Rechnersystemen; Computational Engineering und Robotik; Computer-Netzwerke und verteilte Systeme; Computersystemsicherheit; Informationsmanagement; Software Engineering; Modellierung, Spezifikation und Semantik; Visual Computing.*

    Von den vertiefenden Pflichtveranstaltungen aus 1.b. müssen die Inhalte aus *Computer-Netzwerke und verteilte Systeme; Computersystemsicherheit* im Wesentlichen abgedeckt sein.

2. Unter der Voraussetzung aus Punkt 1 gilt: Sollte das Bachelorstudium des Bewerbers generell Erfahrungen in der oben beschriebenen Form vermitteln, aber die für den Master of Science Studiengang *IT-Sicherheit* wesentlichen Kernfächer der Informatik inhaltlich nicht in hinreichendem Umfang abdecken, kann eine günstige Erfolgsprognose nur dann gestellt und damit zur Sicherung des Studienerfolgs die Zulassung in der Regel nur erteilt werden, wenn sowohl die Abschlussnote als auch der mit CPs gewichtete Durchschnitt der Einzelnoten von Vorlesungen/Übungen und vergleichbaren Lehrveranstaltungsformen im Kernbereich Informatik nicht schlechter als 3,0 ist und jede Einzelnote in diesem Bereich besser als 4,0 ist. In diesem Fall wird das erfolgreiche Absolvieren der Prüfungen in nicht abgedeckten Kernfächern im ersten Studienjahr zur Auflage für die endgültige Zulassung.

3. Bei einem Bachelorstudium, das die oben definierten Anforderungen an die Art der Aufgabenstellung und an die Selbstständigkeit der Bearbeitung nicht erfüllt, kann bei überdurchschnittlichen Prüfungsergebnissen in den Kernfächern der Informatikdavon ausgegangen werden, dass dieser Mangel durch die persönlichen Fähigkeiten des Bewerbers

ausgeglichen werden kann. In diesem Fall kann eine günstige Erfolgsprognose nur dann gestellt und damit die Zulassung nur dann erteilt werden, wenn sowohl die Abschlussnote als auch der mit CPs gewichtete Durchschnitt der Einzelnoten von Vorlesungen/Übungen und vergleichbaren Lehrveranstaltungsformen in den Kernfächern der Informatik 2,0 oder besser ist und zudem keine Einzelnote im Kernbereich Informatik schlechter als 3,0 ist. Für die Auflagen gelten die Regeln von Punkt 3 entsprechend.

Anderweitig gesammelte Erfahrungen (bspw. aus beruflicher Tätigkeit oder aus Weiterbildungskursen) werden in der Eignungsfeststellung für den Master of Science Studiengang *IT-Sicherheit* in vollem Umfang berücksichtigt, sofern sie den oben beschriebenen Erfahrungen sowohl vom Inhalt als auch vom Anspruch an Aufgabenstellung und selbstständige Bearbeitung her entsprechen und wenn diese Kompetenzen unter den allgemein üblichen Qualitätssicherungsstandards von Hochschulen erworben und bewertet worden sind.

1.2.2. Qualifikationsergebnisse

In dem stärker forschungsorientierten Master of Science *IT-Sicherheit* erweitern die Studierenden ihre fachlichen und fachübergreifenden Kompetenzen aus einem vorangegangenen Bachelor-Studiengang. Diese Kompetenzen sind charakteristisch für den Anspruch des Studiengangs und wesentliche Voraussetzung für eine anschließende Promotion. Der Master IT-Sicherheit vermittelt grundlegendes Wissen in den Bereichen der Kryptographie, der Systemsicherheit sowie der Softwaresicherheit. Absolventen des Studienganges können IT-Sicherheitsrisiken erkennen, konkrete Sicherheitsarchitekturen für Hardware- und Softwaresysteme konstruieren und deren Sicherheit bewerten. Nach Abschluss des Studienganges sind die Absolventinnen und Absolventen in der Lage,

- mit ihrer verbesserten Methodenkompetenz komplexe Probleme und Aufgabenstellungen aus dem Bereich der IT-Sicherheit mit wissenschaftlichen Methoden unter Abwägung verschiedener Lösungsansätze selbständig zu bearbeiten,
- diese Kompetenzen auch in neuen und unvertrauten Situationen bei unvollständiger Information umzusetzen und dabei in Systemzusammenhängen zu denken,
- Aufgaben und Probleme mit hohem Abstraktionsvermögen und Blick für komplexe Zusammenhänge zu lösen,
- zukünftige Probleme, Technologien und wissenschaftliche Entwicklungen zu erkennen und bei ihrer Tätigkeit angemessen zu berücksichtigen,
- die Ergebnisse ihrer Analysen bzw. die ausgearbeiteten Lösungen auch an fremdsprachliche Fachleute und Laien zu kommunizieren,
- komplexe Projekte effizient zu organisieren und durchzuführen sowie Teams zielgerichtet zu bilden und zu leiten,
- die gesellschaftliche und ethische Verantwortung ihrer Tätigkeit einzuschätzen und angemessen zu berücksichtigen,
- sich eigenständig fachlich weiterzubilden und weitgehend selbständig wissenschaftlich zu arbeiten.

Zusammenfassend unterscheidet sich der Master-Studiengang von dem vorausgehenden Bachelor-Studiengang vor allem dadurch, dass der Schwerpunkt auf der Lösung komplexer Probleme bei unvollständiger Information liegt, die größeres Abstraktionsvermögen und das Denken in Systemzusammenhängen erfordern. Hinzu kommt verstärkt die Fähigkeit, sich mit der aktuellen Forschungs-

literatur auseinandersetzen zu können sowie die Befähigung zum wissenschaftlichen Arbeiten in einer selbst gewählten Vertiefung und zur selbständigen Lösung aktueller Probleme in der Praxis.

1.3. Anhang III: Modulhandbuch

Das Modulhandbuch wird gemäß § 1 Abs. (1) der *Satzung der Technischen Universität Darmstadt zur Regelung der Bekanntmachung von Satzungen der Technischen Universität Darmstadt* vom 18. März 2010 elektronisch veröffentlicht.