D I E N S T B L A T T
DER HOCHSCHULEN DES SAARLANDES

2016	ausgegeben zu Saarbrücken, 29. September 2016	Nr. 65

UNIVERSITÄT DES SAARLANDES — Seite

Fachspezifische Bestimmungen für den Bachelor-Studiengang Cybersicherheit der Universität des Saarlandes zur Gemeinsamen Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät 6 (Naturwissenschaftlich-Technische Fakultät I – Mathematik und Informatik)

Vom 2. Juni 2016

Die Fakultät 6 (Naturwissenschaftlich-Technische Fakultät I – Mathematik und Informatik) der Universität des Saarlandes hat auf Grund von § 59 Universitätsgesetz vom 23. Juni 2004 (Amtsbl. S. 1782), zuletzt geändert durch Gesetz vom 14. Oktober 2014 (Amtsbl. S. 406), und auf der Grundlage der Gemeinsamen Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät 6 (Naturwissenschaftlich-Technische Fakultät I – Mathematik und Informatik) vom 2. Juli 2015 (Dienstbl. Nr. 72, S. 616), zuletzt geändert durch Ordnung zur Änderung der Gemeinsamen Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät 6 (Naturwissenschaftlich-Technische Fakultät I – Mathematik und Informatik) vom 28. April 2016 (Dienstbl. Nr. 47, S. 404) folgende Fachspezifischen Bestimmungen für den Bachelor-Studiengang Cybersicherheit erlassen, die nach Zustimmung des Senats der Universität des Saarlandes und des Universitätspräsidiums hiermit verkündet werden.

§ 27
Geltungsbereich
(vgl. § 1 Gemeinsame Prüfungsordnung)

Diese Fachspezifischen Bestimmungen gelten für den Bachelor-Studiengang Cybersicherheit der Universität des Saarlandes.

§ 28
Grundsätze
(vgl. § 2 Gemeinsame Prüfungsordnung)

Der Bachelor-Studiengang Cybersicherheit ist stärker forschungsorientiert.

§ 29
Studiengang-Formen
(vgl. § 3 Gemeinsame Prüfungsordnung)

Der Bachelor-Studiengang Cybersicherheit ist ein Kernbereich-Studiengang im Sinne der Rahmenprüfungsordnung der Universität des Saarlandes.

§ 30
Studienaufwand
(vgl. § 4 Gemeinsame Prüfungsordnung)

Für Proseminare, Seminare und Praktika kann eine Anwesenheitspflicht bestehen, die der Dozent zu Beginn der Veranstaltung bekannt gibt.

§ 31
Prüfer/Prüferinnen; Betreuer/Betreuerinnen; Beisitzer/Beisitzerinnen
(vgl. § 8 Gemeinsame Prüfungsordnung)

(1) Der Prüfungsausschuss bestellt Prüfer/Prüferinnen und Gutachter/Gutachterinnen bzw. Betreuer/Betreuerinnen der Bachelor- bzw. Master-Arbeit aus den Gruppen nach § 8 Abs. 1 Nr. 1 bis 7 der gemeinsamen Prüfungsordnung für die Bachelor- und Master-Studiengänge

der Fakultät für Mathematik und Informatik sowie zusätzlich
8. aus der Gruppe der wissenschaftlichen Mitarbeiter mit Promotionsrecht.

(2) Zusätzlich zu den in § 8 Abs. 2 der gemeinsamen Prüfungsordnung genannten Prüfern/Prüferinnen und Gutachtern/Gutachterinnen bzw. Betreuern/Betreuerinnen einer Bachelor- bzw. Master-Arbeit kann der Prüfungsausschuss der Cybersicherheit im Einvernehmen mit den das betreffende Fachgebiet vertretenden Professoren/Professorinnen in besonderen Fällen Leiter/Leiterinnen selbstständiger Nachwuchsgruppen und promovierte Mitglieder der Gruppe der akademischen Mitarbeiter/Mitarbeiterinnen sowie promovierte Mitarbeiter/Mitarbeiterinnen der An-Institute Deutsches Forschungszentrum für Künstliche Intelligenz und der Max-Planck-Institute für Informatik und Softwaresysteme sowie qualifizierte, in der beruflichen Praxis erfahrene Personen bestellen.

§ 32
Verfahren und Gestaltung
(vgl. § 23 Gemeinsame Prüfungsordnung)

Die selbstständige Ausführung der Bachelor- bzw. Master-Arbeit wird in einem 30-minütigen Kolloquium überprüft. Dieses muss spätestens 6 Wochen nach Abgabe der schriftlichen Ausarbeitung der Bachelor- bzw. Master-Arbeit abgelegt werden. Einer der Prüfer soll der Themensteller der Arbeit sein.

§ 33
Akademischer Grad und Abschluss-Dokumente
(vgl. § 25 Gemeinsame Prüfungsordnung)

Das Zeugnis kann über die Angaben nach § 25 Abs. 1 der gemeinsamen Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät für Mathematik und Informatik hinaus weitere erbrachte Leistungen und die jeweils erzielten Ergebnisse enthalten.

§ 34
Inkrafttreten

Diese Ordnung tritt am Tage nach ihrer Bekanntmachung im Dienstblatt der Hochschulen des Saarlandes in Kraft.

Saarbrücken, 29. September 2015

Der Universitätspräsident
(Univ.-Prof. Dr. Volker Linneweber)

Studienordnung der Universität des Saarlandes für den Bachelor-Studiengang Cybersicherheit

Vom 2. Juni 2016

Die Fakultät 6 (Naturwissenschaftlich-Technische Fakultät I – Mathematik und Informatik) der Universität des Saarlandes hat auf Grund von § 54 Universitätsgesetz vom 23. Juni 2004 (Amtsbl. S. 1782), zuletzt geändert durch Gesetz vom 14. Oktober 2014 (Amtsbl. S. 406) und auf der Grundlage der Gemeinsamen Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät 6 (Naturwissenschaftlich-Technische Fakultät I – Mathematik und Informatik) vom 2. Juli 2015 (Dienstbl. Nr. 72, S. 616), zuletzt geändert durch Ordnung zur Änderung der Gemeinsamen Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät 6 (Naturwissenschaftlich-Technische Fakultät I – Mathematik und Informatik) vom 28. April 2016 (Dienstbl. Nr. 47, S. 404) folgende Studienordnung für den Bachelor-Studiengang Cybersicherheit erlassen, die nach Zustimmung des Senats der Universität des Saarlandes hiermit verkündet wird.

§ 1
Geltungsbereich

Diese Studienordnung regelt Inhalt und Aufbau des Bachelor-Studiengangs Cybersicherheit auf der Grundlage der Gemeinsamen Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät 6 (Naturwissenschaftlich-Technische Fakultät I – Mathematik und Informatik) vom 2. Juli 2015 (Dienstbl. Nr. 72, S. 616), zuletzt geändert durch Ordnung zur Änderung der Gemeinsamen Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät 6 (Naturwissenschaftlich-Technische Fakultät I – Mathematik und Informatik) vom 28. April 2016 (Dienstbl. Nr. 47, S. 404) sowie der Fachspezifischen Bestimmungen für den Bachelor-Studiengang Cybersicherheit vom 2. Juni 2016 (Dienstbl. Nr. 65, S. 608). Zuständig für die Organisation von Lehre, Studium und Prüfungen ist die Fakultät für Mathematik und Informatik.

§ 2
Ziele des Studiums und Berufsfeldbezug

(1) Der Bachelor-Studiengang Cybersicherheit verfolgt das Ziel Studierende, aufbauend auf mathematisch-naturwissenschaftlichen Grundlagen, zur Lösung technischer und naturwissenschaftlicher Problemstellungen im Bereich der Cybersicherheit zu befähigen. Darüber hinaus sollen die Absolventen des Bachelor-Studiengangs Cybersicherheit in die Lage versetzt werden, komplexe Fragestellungen auch in allgemeinerem Kontext mit modernen wissenschaftlichen und computergestützten Methoden zu bearbeiten. Neben der wissenschaftlichen Qualifizierung erhalten die Studierenden weiterhin eine praxisorientierte Berufsfähigkeit in Industrie und Wirtschaft. Diese Zielstellungen erfordern eine solide Grundausbildung sowohl in mathematischen Grundlagen als auch in den Grundlagen der Informatik. Zusätzlich wird die Ausbildung durch spezialisierte Veranstaltungen in den verschiedenen Bereichen der Cybersicherheit komplementiert. Ein weiteres wesentliches Element des Cybersicherheits-Studiums ist die Anwendung von vermittelten theoretischen Grundlagen im Rahmen von Praktika und Projekten.

(2) Die akademische Ausbildung mit dem Abschluss B.Sc. in Cybersicherheit liefert eine hinreichende Voraussetzung für weitere fachverwandte Master-Studiengänge.

§ 3
Studienbeginn und Studiendauer

(1) Das Studium kann jeweils zum Winter- und Sommersemester eines Jahres aufgenommen werden. Der Start zum Wintersemester wird empfohlen.

(2) Das Lehrangebot ist so organisiert, dass das Studium in sechs Semestern abgeschlossen werden kann (Regelstudienzeit).

§ 4
Art der Lehrveranstaltungen

Das Lehrangebot wird durch Lehrveranstaltungen folgender Art vermittelt:

1. Vorlesungen (V): Sie dienen zur Einführung in ein Fachgebiet und vermitteln u. a. einen Überblick über fachtypische theoretische Konzepte und Prinzipien, Methoden und Fertigkeiten, Technologien und praktische Realisierungen. Vorlesungen geben Hinweise auf weiterführende Literatur und eröffnen den Weg zur Vertiefung der Kenntnisse durch Übungen, Praktika und ergänzendes Selbststudium.

2. Übungen (Ü): Sie finden überwiegend als Ergänzungsveranstaltungen zu Vorlesungen bevorzugt in kleineren Gruppen statt. Sie sollen den Studierenden durch Bearbeitung exemplarischer Probleme die Gelegenheit zur Anwendung und Vertiefung der in der Vorlesung vermittelten Lehrinhalte sowie zur Selbstkontrolle des Wissensstandes ggf. durch eigene Fragestellung geben.

3. Seminare (S) erweitern die bereits erworbenen Kenntnisse und vermitteln durch das Studium von Fachliteratur und Quellen in Seminargesprächen, Referaten oder Seminararbeiten einen vertieften Einblick in einen Forschungsbereich. Sie dienen darüber hinaus dem Erlernen wissenschaftlicher Darstellungs- und Vortragstechniken sowie der Anleitung zu kritischer Sachdiskussion von Forschungsergebnissen. Zusätzlich können projektbezogene Arbeiten zu aktuellen wissenschaftlichen Diskussionen vorgesehen sein. Die dabei vertieften Inhalte können in einem Bachelorseminar die Grundlage für die Bachelorarbeit bilden.

4. Praktikum und Projekte (P): In einem Praktikum oder Projekt werden fachpraktische Themen angeboten, die in die spezifische Arbeitsweise der betreffenden Studienfächer einführen. Die den Themen zugrunde liegenden theoretischen Kenntnisse erwirbt man durch Vorlesungen und Literaturstudien. Ein weiteres Ziel der Praktika ist die Vermittlung computergestützter Methoden durch praktische Anwendung. In Projekten werden in der Regel fachübergreifende Themen behandelt. Die Bearbeitung eines Themas bietet den Studierenden die Gelegenheit, in Gruppen unter Anleitung themenspezifische Aufgabenstellungen von der Konzeption bis hin zur praktischen Realisierung zu lösen. Man lernt hier einerseits die Zusammenhänge zwischen Theorie und Praxis durch eigene selbstständige Arbeit kennen, andererseits wird die Gruppenarbeit in Projekten gefördert. Teilnahme an Praktika oder Projekten kann vom Nachweis über die erfolgreiche Teilnahme an zugehörigen Vorlesungen und Übungen abhängig gemacht werden.

§ 5
Aufbau und Inhalte des Studiums

(1) Das Studium des Bachelor-Studiengangs Cybersicherheit umfasst eine Gesamtleistung von 180 Credit Points (CP) nach dem European Credit Transfer System (ECTS). Davon müssen die Vorlesungen des Pflichtbereichs (§ 5 Abs. 2 Nr. 1, ausgenommen das Softwarepraktikum, und § 5 Abs. 2 Nr. 2) und der Wahlpflichtbereich I (§ 5 Abs. 2 Nr. 3.) als benotete Leistungen erbracht werden. Der Wahlpflichtbereich II (§ 5 Abs. 2 Nr. 4.) ist unbenotet. Pro Semester sind in der Regel 30 CP zu erwerben.

(2) Das Studium umfasst Module zu folgenden Teilbereichen. Die Module und Modulelemente der einzelnen Teilbereiche, sowie jeweils die Art der Lehrveranstaltung, deren Semesterwochenstunden und Credit Points, Zyklus, sowie die Art der Prüfung und Benotung sind in Anhang A beschrieben.

1. den Pflichtbereich mit den Modulen: „Programmierung 1 & 2“ (jeweils 9 CP), „Mathematik für Informatiker 1 & 2“ (jeweils 9 CP), „Systemarchitektur“ (9 CP), „Grundzüge der Theoretischen Informatik“ (9 CP), „Softwarepraktikum“ (9 CP), „Grundzüge von Algorithmen & Datenstrukturen“ (6 CP), „Nebenläufige Programmierung“ (6 CP), „Informationssysteme“ (6 CP), „Proseminar“ (5 CP), „Seminar“ (7 CP), „Bachelor-Seminar“ (9 CP) und „Bachelor-Arbeit“ (12 CP) aus dem Fachbereich der Informatik.

2. den spezialisierten Pflichtbereich mit den Modulen: „Grundlagen der Cybersicherheit 1“ (9 CP), „Grundlagen der Cybersicherheit 2“ (6 CP), „Security“ (9 CP), „Cryptography“ (9 CP), und „Cybersicherheitsprojekt (9 CP) aus dem Fachbereich der Informatik.

3. Den „Wahlpflichtbereich I“ (18 CP) mit wählbaren Modulen aus der Liste der Vertiefungsvorlesungen der Cybersicherheit (Anhang A). Die Liste der Vertiefungsvorlesungen der Cybersicherheit gemäß Anhang A kann durch den Prüfungsausschuss modifiziert werden.

4. Den “Wahlpflichtbereich II” (mind. 6 CP) mit wählbaren Modulen aus den Bereichen:

   a) Kursangebote aus dem Fachbereich der Informatik,
   b) Betreuung von Übungsgruppen (Tutortätigkeit); in der Regel je 4 CP, wobei eine mehrfache Erbringung dieser Leistungen möglich ist, sofern die Übungsgruppen unterschiedlichen Modulen angehören,
   c) Sprachkurse (maximal 6 CP; lebende Sprache; nicht die Muttersprache,
   d) Soft Skill Seminar,
   e) Industrie-Praktikum (maximal 6 CP), das auf Antrag an den Prüfungsausschuss genehmigt wurde,
   f) Module, die auf Antrag an den Prüfungsausschuss genehmigt wurden. Studierende haben beispielsweise die Möglichkeit, einen Antrag an den Prüfungsausschuss auf Anerkennung des geleisteten studentischen Engagements (insbesondere Mitarbeit bei der akademischen Selbstverwaltung) sowie Veranstaltungen zu Schlüssel-qualifikationen im Umfang von jeweils maximal 3 CP zu stellen.

(3) Im Pflichtbereich sind alle in § 5 Abs. 2 Nr. 1 und Nr. 2 genannten Module zu belegen. Im Wahlpflichtbereich können gesamte Module oder einzelne Lehrveranstaltungen belegt werden.

(4) Im Pflichtbereich werden insgesamt 156 CP erworben (12 CP davon entfallen auf das Modul „Bachelor-Arbeit“ und 9 CP auf das Modul „Bachelor-Seminar“) und im Wahlpflichtbereich sind mindestens 24 CP zu erwerben.

(5) Bei Veranstaltungen aus den Bereichen Praktikum, Proseminar und Seminar sowie in den Modulen "Tutor", "Soft Skill Seminar" und "Sprachkurse" aus dem Wahlpflichtbereich stehen begrenzte Teilnehmerplätze, abhängig von der entsprechenden Veranstaltung zur Verfügung. Die Zulassung wird durch den Modulverantwortlichen geregelt.

(6) Eine Prüfungsleistung ist entweder benotet oder unbenotet einzubringen. Die Teilung einer benoteten Prüfungsleistung in unbenotete und benotete Credit Points ist nicht möglich.

(7) Für folgende Veranstaltungen aus § 5 Abs. 2 Nr. 1 und 2, „Programmierung 1 & 2“, „Mathematik für Informatiker 1 & 2“, „Systemarchitektur“, „Grundzüge der Theoretischen Informatik“, „Grundzüge von Algorithmen & Datenstrukturen“, „Nebenläufige Programmierung“, „Informationssysteme“, „Grundlagen der Cybersicherheit 1“ und „Grundlagen der Cybersicherheit 2“, wird einmalig eine nicht bestandene Prüfungsleistung, die beim erstmöglichen Prüfungstermin und vor Ablauf des Regelstudiensemesters abgelegt wird, als „Freiversuch“ gewertet (vgl. § 17 Abs. 4 der Prüfungsordnung), falls die Prüfungsleistung unmittelbar, d.h. im gleichen Prüfungszeitraum (vgl. § 13 Abs. 4 der Prüfungsordnung) wiederholt wird. Das Regelstudiensemester für die Veranstaltungen nach § 5 Abs. 2 Nr. 1 und 2 beträgt 6.

(8) Eine bestandene Prüfungsleistung folgender Veranstaltungen aus § 5 Abs. 2, Nr. 1 und 2, „Programmierung 1 & 2“, „Mathematik für Informatiker 1 & 2“, „Systemarchitektur“, „Grundzüge der Theoretischen Informatik“, „Grundzüge von Algorithmen & Datenstrukturen“, „Nebenläufige Programmierung“, „Informationssysteme“, „Grundlagen der Cybersicherheit 1“ und „Grundlagen der Cybersicherheit 2“ sowie der Stammvorlesungen („Security“ und „Cryptography“) kann in der Regelstudienzeit einmalig zur Notenverbesserung im gleichen Prüfungszeitraum (vgl. § 13 Abs. 4 der Prüfungsordnung) wiederholt werden. Bestandene Prüfungsleistungen der Vertiefungsvorlesungen können einmalig zur Notenverbesserung im gleichen Prüfungszeitraum wiederholt werden, falls der Dozent zu Beginn der Veranstaltung die jeweilige Prüfungsleistung als verbesserbar ausweist. Dabei zählt das bessere Ergebnis. Ansonsten ist die Wiederholung einer bestandenen Prüfungsleistung nicht zulässig.

(9) Die Module der Pflichtbereiche werden mindestens einmal im Jahr angeboten. Es wird sichergestellt, dass in jedem Semester mindestens zwei Module aus dem Wahlpflichtbereich I angeboten werden. Proseminare, Seminare und Vertiefungsvorlesungen können einmalig angeboten werden. Der Studiendekan/Die Studiendekanin stellt in jedem Studienjahr ein hinreichendes Angebot sicher.

(10) Die Unterrichtssprache ist in den Grundlagenveranstaltungen des Bachelor-Studiengangs in der Regel Deutsch, in den weiterführenden Vorlesungen und Wahlpflichtbereichen Englisch. Die Unterrichtssprache wird zu Beginn der Veranstaltungen bekannt gegeben.

(11) Das Studienangebot in den verschiedenen Wahlpflichtmodulbereichen kann für ein oder mehrere Semester modifiziert werden, wobei dies vom Prüfungsausschuss zu genehmigen ist. Diese Veranstaltungen, ihr Gewicht in CP und ihre Zugehörigkeit zu den Modulbereichen werden jeweils vor Semesterbeginn bekannt gegeben.

(12) Detaillierte Informationen zu den Inhalten der Module und Modulelemente werden im Modulhandbuch beschrieben, das in geeigneter Form bekannt gegeben wird. Änderungen an

den Festlegungen des Modulhandbuchs, die nicht in dieser Studienordnung geregelt sind, sind dem zuständigen Studiendekan/der zuständigen Studiendekanin anzuzeigen und in geeigneter Form zu dokumentieren.

(13) Für Proseminare, Seminare, Übungen und Praktika kann eine Anwesenheitspflicht bestehen, die der Dozent zu Beginn der Veranstaltung bekannt gibt.

§ 6
Studienplan

Der Studiendekan/die Studiendekanin erstellt auf der Grundlage dieser Studienordnung einen Studienplan, der nähere Angaben über Art und Umfang der Modulelemente (Anhang A) enthält sowie Empfehlungen für einen zweckmäßigen Aufbau des Studiums gibt (Anhang B). Dieser wird in geeigneter Form bekannt gegeben. Das jeweils aktuelle Modulelementangebot in den verschiedenen Modulkategorien wird im Vorlesungsverzeichnis des jeweiligen Semesters bekannt gegeben.

§ 7
Studienberatung

(1) Die Zentrale Studienberatung der Universität des Saarlandes berät Interessierte und Studierende über Inhalt, Aufbau und Anforderungen eines Studiums. Darüber hinaus gibt es Beratungsangebote bei Entscheidungsproblemen, bei Fragen der Studienplanung und Studienorganisation.

(2) Fragen zu Studienanforderungen und Zulassungsvoraussetzungen, zur Studienplanung und -organisation beantwortet der Fachstudienberater/die Fachstudienberaterin für den Studiengang Cybersicherheit.

(3) Für spezifische Rückfragen zu einzelnen Modulen stehen die Modulverantwortlichen zur Verfügung.

§ 8
Auslandsaufenthalt

Es besteht die Möglichkeit, ein Auslandsstudium zu absolvieren. Die Studierenden sollten an einer Beratung zur Durchführung des Auslandsstudiums teilnehmen, ggf. vorbereitende Sprachkurse belegen und im Vorfeld über ein Learning Agreement die Anerkennung von Studienleistungen gemäß der einschlägigen Prüfungsordnung klären. Über Studienmöglichkeiten, Austauschprogramme, Stipendien und Formalitäten informieren sowohl das International Office als auch die Fachvertreter des entsprechenden Schwerpunktfachs. Aufgrund langer Antragsfristen und Bearbeitungszeiten bei ausländischen Universitäten wie Stipendiengebern sollte die Anmeldung für ein Auslandsstudium in der Regel ein Jahr vor Antritt des Auslandaufenthalts im Prüfungssekretariat erfolgen.

§ 9
Bachelor-Arbeit und Bachelor-Seminar

(1) Durch die Anfertigung einer Bachelor-Arbeit soll der/die Studierende nachweisen, dass er/sie theoretisch-konzeptuelle und/oder angewandte Aufgabenstellungen aus dem Bereich der Cybersicherheit oder verwandten Bereichen eigenständig bearbeiten kann. Die Bearbeitungszeit beträgt drei Monate. Der mit der Bachelorarbeit verbundene Aufwand wird mit 12 CP kreditiert.

(2) Jeder Studierende muss vor Abschluss der Bachelor-Arbeit erfolgreich ein Bachelor-Seminar mit direktem Bezug zu dem Thema der Bachelor-Arbeit abgeschlossen haben. Dieses beinhaltet sowohl einen Vortrag über die geplante Themenstellung als auch eine schriftliche Beschreibung der geplanten Aufgabenstellung der Bachelor-Arbeit.

(3) Die Bachelor-Arbeit muss spätestens ein Semester nach erfolgreicher Teilnahme am Bachelor-Seminar beim Prüfungssekretariat angemeldet werden. Nach Ablauf dieser Frist muss erneut ein Bachelor-Seminar erfolgreich absolviert werden.

§ 10
Inkrafttreten

Diese Ordnung tritt am Tage nach ihrer Bekanntmachung im Dienstblatt der Hochschulen des Saarlandes in Kraft.

Saarbrücken, 29. September 2016

Der Universitätspräsident
Univ.-Prof. Dr. Volker Linneweber

Anhang A. Module und Prüfungsleistungen Bachelor-Cybersicherheit

Bachelor-Studiengang (B.Sc.) "Cybersicherheit"					WS		SS		WS		SS		WS		SS	
Modulkategorie- bzw. Modulbezeichnung	**Modulelement**	**Art der Prüfung**			**Fachsemester**											
					1		2		3		4		5		6	
			CP (ECTS) mit Note	**CP (ECTS)** unbenotet	V / Ü / P SWS	CP	V / Ü / P SWS	CP	V / Ü / P SWS	CP	V / Ü / P SWS	CP	V / Ü / P SWS	CP	V / Ü / P SWS	CP
Grundlagen der Cybersicherheit 1		Klausur(en), PVL	**9**		**2 / 2 / 2**	**9**										
Mathematik für Informatiker 1		Klausur(en), PVL	**9**		**4 / 2 / 0**	**9**										
Programmierung 1		Klausur(en), PVL	**9**		**4 / 2 / 0**	**9**										
Mathematik für Informatiker 2		Klausur(en), PVL	**9**				**4 / 2 / 0**	**9**								
Programmierung 2		Klausur(en), PVL	**9**				**4 / 2 / 0**	**9**								
Grundlagen der Cybersicherheit 2		Klausur(en), PVL	**6**				**2 / 2 / 0**	**6**								
Systemarchitektur		Klausur(en), PVL	**9**				**4 / 2 / 0**	**9**								
Softwarepraktikum		Projektarbeit		**9**					**1 / 1 / 4**	**9**						
Grundzüge der Theoretischen Informatik		Klausur(en), PVL	**9**						**4 / 2 / 0**	**9**						
Grundzüge von Algorithmen und Datenstrukturen		Klausur(en), PVL	**6**						**2 / 2 / 0**	**6**						
Cryptography		Klausur(en), PVL	**9**						**4 / 2 / 0**	**9**						
Proseminar		mündlich, schriftlich	**5**								**0 / 0 / 2**	**5**				
Security		Klausur(en), PVL	**9**								**4 / 2 / 0**	**9**				
Informationssysteme		Klausur(en), PVL	**6**								**2 / 2 / 0**	**6**				
Nebenläufige Programmierung		Klausur(en), PVL	**6**								**2 / 2 / 0**	**6**				
Cybersicherheitsprojekt		Projektarbeit	**9**										**0 / 0 / 6**	**9**		
Seminar		mündlich, schriftlich	**7**										**0 / 0 / 3**	**7**		
Vertiefungsvorlesungen Cybersicherheit I (Wahlpflicht I)		Klausur(en), PVL	**6**										**2 / 2 / 0**	**6**		
Vertiefungsvorlesungen Cybersicherheit II (Wahlpflicht I)		Klausur(en), PVL	**6**										**2 / 2 / 0**	**6**		
Vertiefungsvorlesungen Cybersicherheit III (Wahlpflicht I)		Klausur(en), PVL	**6**												**2 / 2 / 0**	**6**
Angebot Vertiefungsvorlesungen Cybersicherheit (Wahlpflicht I, Umfang min. 18 CP): Alle Vorlesungen 2 / 2 / 0 mit jeweils 6 CP																
	Privacy-Enhancing Cryptography	Klausur(en), PVL														
	Advanced Cryptography	Klausur(en), PVL														
	Malware Analysis and Intrusion Detection	Klausur(en), PVL														
	Theoretical Foundation of Cyber Security	Klausur(en), PVL														
	Web and Mobile Security	Klausur(en), PVL														
	Cyber Attacks and Defenses	Klausur(en), PVL														
Prüfungsausschuss kann das Studienangebot modifizieren																
Wahlpflicht II (Umfang min. 6CP)				**6**												
Tutor		Tutortätigkeit									**0 / 3 / 0**	**4**				
Soft Skill Seminar		mündlich, schriftlich														
Sprachkurs		mündlich, schriftlich														
Industriepraktikum (max. 6 CP)																
Ringvorlesung: Perspektiven der Informatik		schriftlich			**2 / 0 / 0**	**2**										
Weitere Vorlesungen aus dem Fachbereich Informatik		mündlich, schriftlich														
Prüfungsausschuss kann das Studienangebot modifizieren																
Abschlussarbeit **(21 CP)**																**21**
Bachelor-Seminar		mündlich, schriftlich	9												**0 / 0 / 5**	**9**
Bachelor-Arbeit		Bachelorarbeit	12													**12**
	Summe **CP (ECTS) gesamt**		**165**	**15**	**12 / 6 / 2**	**29**	**14 / 8 / 0**	**33**	**11 / 7 / 4**	**33**	**8 / 9 / 2**	**30**	**4 / 4 / 9**	**28**	**2 / 2 / 5**	**27**

Legende: V = Vorlesung, Ü = Übung, P = Projekt oder Praktikum, PVL = Prüfungsvorleistung, CP = Credit Points, SWS = Semesterwochenstunden

Anhang B. Beispielstudienplan Bachelor-Cybersicherheit

§ 1
Allgemeiner Aufbau

1	Programmierung 1 (9 CP)	Mathematik für Informatiker 1 (9 CP)	Grundlagen der Cybersicherheit 1 (9 CP)	Ringvorlesung (2 CP)		29
2	Programmierung 2 (9 CP)	Mathematik für Informatiker 2 (9 CP)	Grundlagen der Cybersicherheit 2 (6 CP)	Systemarchitektur (9 CP)		33
3	Cryptography (9 CP)	Grundzüge der Theoretischen Informatik (9 CP)	Grundzüge von Algorithmen und Datenstrukturen (6 CP)	Software Praktikum (9 CP)		33
4	Security (9 CP)	Proseminar (5 CP)	Nebenläufige Programmierung (6 CP)	Informations-systeme (6 CP)	Tutor (4 CP)	30
5	Cybersicherheitsprojekt (9 CP)	Seminar (7 CP)	Vertiefung I - Cybersicherheit (6 CP)	Vertiefung II - Cybersicherheit (6 CP)		28
6	Bachelor Arbeit (12 CP)	Bachelor Seminar (9 CP)	Vertiefung III - Cybersicherheit (6 CP)			27