

Fachprüfungsordnung für den Masterstudiengang Cyber-Sicherheit

**der Universität der Bundeswehr München
(FPOCYB/Ma)**

**vom 29. September 2017
geändert durch Änderungssatzung vom 21. April 2020
und durch Änderungssatzung vom 23. Januar 2025**

Konsolidierte Lesefassung*

***Hinweis:**

Bei der vorliegenden Fassung der FPOCYB/Ma handelt es sich um eine nicht amtliche Lesefassung, in der in die Version der FPOCYB/Ma vom 29. September 2017 die durch die Änderungssatzungen vom 21. April 2020 und vom 23. Januar 2025 vorgenommenen Änderungen eingearbeitet sind. Dadurch soll für die Studierenden eine bessere Lesbarkeit erreicht werden.

Der Text dieser Satzung wurde sorgfältig erstellt; gleichwohl können Übertragungsfehler nicht ausgeschlossen werden und es sind nur die amtlichen Veröffentlichungen der FPOCYB/Ma vom 29. September 2017 und der Änderungssatzungen vom 21. April 2020 und vom 23. Januar 2025 unter dem Link: <https://publicwiki.unibw.de/display/DAT/Satzungen+und+Ordnungen+der+UniBw+M> und in den Allgemeinen Bekanntmachungen der Universität der Bundeswehr München/Amtliches Mitteilungsblatt rechtlich verbindlich:

- 1.) Allgemeine Bekanntmachungen der Universität der Bundeswehr München vom 13. November 2017 / Amtliches Mitteilungsblatt Nr. 4/2017, S. 4, lfd. Nr. 5, Anlage 5: FPOCYB/Ma vom 29. September 2017.
- 2.) Allgemeine Bekanntmachungen der Universität der Bundeswehr München vom 15. Mai 2020 / Amtliches Mitteilungsblatt Nr. 2/2020, S. 4, lfd. Nr. 6, Anlage 6: Änderungssatzung der FPOCYB/Ma vom 21. April 2020.
- 3.) Allgemeine Bekanntmachungen der Universität der Bundeswehr München vom 4. März 2025 / Amtliches Mitteilungsblatt Nr. 1/2025, S. 4, lfd. Nr. 3, Anlage 3: Zweite Änderungssatzung der FPOCYB/Ma vom 23. Januar 2025.

Fachprüfungsordnung
für den
universitären Masterstudiengang

Cyber-Sicherheit

der
Universität der Bundeswehr München
(FPOCYB/Ma)

vom 29. September 2017

in der Fassung der

1. Änderungssatzung vom 21. April 2020

und der

2. Änderungssatzung vom 23. Januar 2025

Aufgrund von Art. 82 Sätze 3 und 4 sowie Art. 80 Abs. 1 und 3 in Verbindung mit Art. 61 Abs. 2 Satz 1 des Bayerischen Hochschulgesetzes (BayHSchG) erlässt die Universität der Bundeswehr München (UniBw M) folgende Fachprüfungsordnung:

Inhaltsübersicht

Seite

A Allgemeine Bestimmungen

§ 1 Geltungsbereich 4

§ 2 Zugang zum Masterstudiengang 4

B Studienverlauf

§ 3 Vertiefungsfelder und Module des
Masterstudiengangs 4

§ 4 Master-Arbeit 5

C Akademischer Grad und Zeugnis

§ 5 Master-Grad 5

§ 6 Zeugnis 5

D Schlussbestimmungen

§ 7 In-Kraft-Treten 6

Anlage 1: Übersicht über die Module und
Leistungsnachweise 7

Anlage 2: Niederschrift zum
Qualifizierungsgespräch
gemäß § 24 Abs. 2 ABaMaPO 10

Anlage 3: Verzeichnis verwendeter
Abkürzungen 11

A
Allgemeine Bestimmungen

§ 1
Geltungsbereich
(zu § 1 ABaMaPO)

Diese Fachprüfungsordnung für den universitären Masterstudiengang Cyber-Sicherheit (FPOCYB/Ma) ergänzt die Allgemeine Prüfungsordnung für die universitären Bachelor- und Master-Studiengänge der Universität der Bundeswehr München (ABaMaPO) in der jeweils geltenden Fassung im Hinblick auf die besonderen Gegebenheiten und Anforderungen des universitären Masterstudiengangs Cyber-Sicherheit (CYB/Ma).

§ 2
Zugang
zum Masterstudiengang
(zu § 28 ABaMaPO)

(1) Voraussetzung für den Zugang zum Masterstudiengang ist der Abschluss des Bachelorstudiengangs Informatik der UniBw M oder der Abschluss eines der Bachelorstudiengänge Wirtschaftsinformatik oder Mathematical Engineering der UniBw M oder ein abgeschlossenes natur- oder ingenieurwissenschaftliches oder mathematisches Hochschulstudium, das in Umfang, Inhalt und Ausrichtung einem dieser Bachelorstudiengänge mindestens gleichwertig ist. ²Zudem ist der Nachweis von Kenntnissen der englischen Sprache auf dem Level des Sprachleistungsprofils (SLP) 3332 oder von B 2 des gemeinsamen europäischen Referenzrahmens für Sprachen oder eines vergleichbaren Sprachniveaus erforderlich.

(2) Liegt ein Fall des § 28 Abs. 2 ABaMaPO vor, muss die bzw. der Studierende die studien-gangsspezifische Eignung durch die erfolgreiche Absolvierung eines Qualifizierungsgesprächs nach den näheren Bestimmungen der Anlage 3 nachweisen.

B
Studienverlauf

§ 3
Vertiefungsfelder und Module des
Masterstudiengangs
(zu §§ 5, 29 ABaMaPO)

(1) ¹Die für den Masterstudiengang Cyber-Sicherheit angebotenen Module sind mit den zugehörigen ECTS-Leistungspunkten in der Anlage 1 angegeben. ²Jede bzw. jeder Studierende absolviert die Pflicht- und Wahlpflichtmodule sowie das Modul Seminar gemäß Anlage 1, Tabellen 1 bis 3 und das Modul Master-Arbeit gemäß Anlage 1, Tabelle 4 sowie die Module des Begleitstudiums *studium plus* gemäß Anlage 1, Tabelle 5.

(2) ¹Der Masterstudiengang Cyber-Sicherheit kann in den Vertiefungsfeldern:

- Enterprise Security
- Public Security
- Security Intelligence
- Cyber Network Capabilities

studiert werden. ²Dazu sind die Wahlpflichtmodule im Modulhandbuch einem oder mehreren der Vertiefungsfelder zugeordnet.

§ 4 Master-Arbeit (zu § 31 ABaMaPO)

¹Jede bzw. jeder Studierende fertigt im Masterstudiengang Cyber-Sicherheit eine Master-Arbeit an. ²Die Regelbearbeitungszeit für die Master-Arbeit beträgt fünf Monate. ³Die Master-Arbeit hat einen Umfang von 30 ECTS-Leistungspunkten. ⁴Sie ist spätestens 13 Monate nach Aufnahme des Masterstudiengangs zu beginnen. ⁵Die Masterarbeit ist in einer ca. 15- bis 30-minütigen Darstellung vor der Themenstellerin bzw. dem Themensteller zu präsentieren.

C Akademischer Grad und Zeugnis

§ 5 Master-Grad (zu §§ 32 ABaMaPO)

¹Aufgrund der bestandenen Master-Prüfung wird der akademische Grad "Master of Science", abgekürzt "M.Sc.", verliehen. ²Der akademische Grad kann mit dem Hochschulzusatz "(UniBw M)" geführt werden.

§ 6 Zeugnis (zu § 22 ABaMaPO)

¹Über die bestandene Master-Prüfung wird ein Zeugnis ausgestellt, das die in den Modulen erzielten Noten, das Thema sowie die Note der Master-Arbeit und die Master-Note enthält. ²Im Zeugnis wird zusätzlich auf Grund des Prüfungsgesamtergebnisses eine relative Note nach dem ECTS Users' Guide ausgewiesen. ³Als Grundlage für die Berechnung der relativen Note werden die letzten drei Studienjahrgänge als Kohorte erfasst. ⁴Sind 18 oder mehr Leistungspunkte aus den gemäß § 3 Abs. 1 i.V.m. Anlage 1 Tabelle 2 erforderlichen Wahlpflichtmodulen durch Module abgedeckt, die einem der in § 3 Abs. 2 genannten Vertiefungsfelder zugeordnet sind, dann wird dem/der Studierenden dieses Vertiefungsfeld im Zeugnis durch einen Zusatz bestätigt. ⁵Wenn die in Satz 4 genannte Voraussetzung für mehr als ein Vertiefungsfeld erfüllt ist, dann ist eines davon für die Bestätigung auszuwählen. ⁶Auf Antrag kann der Zusatz für das Vertiefungsfeld entfallen.

D
Schlussbestimmungen

§ 7
In-Kraft-Treten

Fachprüfungsordnung vom 29. September 2017

¹Diese Fachprüfungsordnung tritt am 1. Januar 2018 in Kraft. ²Sie findet erstmals Anwendung auf Studierende, die den Masterstudiengang am 1. Januar 2018 beginnen.

1. Änderungssatzung vom 21. April 2020

¹Diese Änderungssatzung tritt mit Wirkung vom 1. Januar 2020 in Kraft. ²Sie findet erstmals Anwendung auf Studierende, die ihr Studium am 1. Januar 2020 begonnen haben.

2. Änderungssatzung vom 23. Januar 2025

¹Diese Änderungssatzung tritt mit Wirkung vom 1. Januar 2025 in Kraft. ²Sie findet erstmals Anwendung auf Studierende, die ihr Studium am 1. Januar 2025 begonnen haben.

Universität der Bundeswehr München
Univ.-Prof. Dr. Merith Niehuss
Präsidentin

Anlage 1: Übersicht über die Module und Leistungsnachweise

Die konkreten Veranstaltungsformen der Teilveranstaltungen zu den jeweiligen Modulen können dem Modulhandbuch zum Masterstudiengang Cyber-Sicherheit entnommen werden, das vom Fakultätsrat der Fakultät für Informatik verabschiedet und jährlich fortgeschrieben wird. Sind für den Leistungsnachweis in dieser Anlage zur Fachprüfungsordnung bei einem Modul alternative Formen zugelassen, so kann die tatsächlich verwendete Prüfungsform ebenfalls dem Modulhandbuch entnommen werden.

Tabelle 1: Pflichtmodul

Alle Studierenden des Studiengangs CYB/Ma haben folgende im Modulhandbuch näher ausgeführte Pflichtmodule erfolgreich abzuschließen:

Modul	ECTS-Leistungspunkte	Leistungsnachweis	Regeltermine der Leistungsnachweise
Netzsicherheit	6	sP-60-120 oder mP-20-30 oder Pf (Bearbeitungszeitraum 14 bis 26 Wochen)	2. Trimester
Hardwaresicherheit	6	sP-60-120 oder mP-20-30 oder Pf (Bearbeitungszeitraum 14 bis 26 Wochen)	2. Trimester
Datenschutz und Privacy	6	sP-60-120 oder mP-20-30 oder Pf (Bearbeitungszeitraum 6 bis 12 Wochen)	1. oder 4. Trimester
Systemsicherheit	6	sP-60-120 oder mP-20-30 oder Pf (Bearbeitungszeitraum 6 bis 12 Wochen)	2. Trimester
Kryptologie	6	sP-60-120 oder mP-20-30 oder Pf (Bearbeitungszeitraum 6 bis 12 Wochen)	1. Trimester
Anwendungssicherheit	6	sP-60-120 oder mP-20-30 oder Pf (Bearbeitungszeitraum 6 bis 12 Wochen)	2. Trimester
Security- und IT-Management	8	sP-60-120 oder mP-20-30 oder Pf (Bearbeitungszeitraum 6 bis 12 Wochen)	3. Trimester
Summe	44		

Studierenden, die im Bachelorstudium noch nicht das Modul „Grundlagen der Informationssicherheit“ oder ein inhaltsgleiches Modul absolviert haben, wird dringend empfohlen, zusätzlich das folgende Pflichtmodul „Grundlagen der Informationssicherheit“ im Umfang von 6 ECTS-Leistungspunkten am Anfang des Masterstudiums Cyber-Sicherheit zu belegen. Damit erhöht sich die Summe der Pflichtmodule auf 50 ECTS-Leistungspunkte.

Modul	ECTS-Leistungspunkte	Leistungsnachweis	Regeltermine der Leistungsnachweise
Grundlagen der Informationssicherheit	6	sP-60-120 oder mP-20-30 oder Pf (Bearbeitungszeitraum 6 bis 12 Wochen)	1. Trimester

Tabelle 2: Wahlpflichtmodule

Die Wahlpflichtmodule sind jeweils einem oder mehreren der folgenden Vertiefungsfelder zugeordnet:

- Enterprise Security
- Public Security
- Security Intelligence
- Cyber Network Capabilities

Aus den Wahlpflichtmodulen sind von den Studierenden Module im Umfang von insgesamt mindestens 36 ECTS-Leistungspunkten zu absolvieren, wenn nach Tabelle 1 Pflichtmodule im Umfang von insgesamt 44 ECTS-Leistungspunkten belegt werden. Wenn nach Tabelle 1 Pflichtmodule im Umfang von insgesamt 50 ECTS-Leistungspunkten belegt werden, sind Wahlpflichtmodule im Umfang von insgesamt mindestens 30 ECTS-Leistungspunkten zu absolvieren. Werden 18 oder mehr der ECTS-Leistungspunkte im Wahlpflichtbereich durch Module abgedeckt, die alle demselben Vertiefungsfeld zugeordnet sind, dann wird dieses Vertiefungsfeld im Abschlusszeugnis bestätigt (§ 7).

Modul	ECTS-Leistungspunkte	Leistungsnachweis	Regeltermine der Leistungsnachweise
Wahlpflichtmodule gemäß Modulhandbuch	jew. 3, 5, 6, 9 oder 12	jew. sP-60-120 oder mP-20-40 oder Pf (Bearbeitungszeitraum: pro Trimester 6 bis 12 Wochen)	1.-5. Trimester
Rechtliche Grundlagen Cyber Network Capabilities	6	HA (Bearbeitungszeitraum 3 bis 4 Wochen)	1.-5. Trimester

Tabelle 3: Seminar

Modul	ECTS-Leistungspunkte	Art der Lehrveranstaltung	Leistungsnachweis	Regeltermine der Leistungsnachweise
Seminar	5	S	Ref (30 bis 60 Minuten) oder SemA mit Vortrag (20 bis 40 Minuten), Bearbeitungszeit jeweils 100 bis 140 Stunden	2.-5. Trimester

Tabelle 4: Master-Arbeit

Modul	ECTS-Leistungspunkte	Leistungsnachweis	Regeltermine der Leistungsnachweise
Master-Arbeit	30	gemäß §§ 26 und 31 ABaMaPO	4.-5. Trimester

Tabelle 5: verpflichtendes Begleitstudium *studium plus*

Modul	ECTS-Leistungspunkte	Art der Lehrveranstaltung	Leistungsnachweis	Regeltermine der Leistungsnachweise
<i>studium plus</i> 3, Seminar und Training	5	S, V, Ü, T	SemA, Pf, TS	1.-5. Trimester

Anlage 2: Niederschrift zum Qualifizierungsgespräch gemäß § 28 Abs. 2 ABaMaPO

Name der/des Studierenden, Matr. Nr.: _____
 Namen der Kommissionsmitglieder: _____

Ort, Datum und Dauer des Gesprächs: _____

1. Verlauf des Gesprächs:

(wesentliche Themen des Gesprächs und Gründe für die Beurteilung):

2. Studiengangsspezifische Beurteilungskriterien:

Im Verlauf des Gesprächs wurden folgende Beurteilungskriterien geprüft und bewertet:

Nr.	Beurteilungskriterien	Max. ¹	Ist
1	Verständnis für grundlegende Fragestellungen der Cyber-Sicherheit	25	
2	Fähigkeit zu wissenschaftlicher bzw. grundlagenmethodischer Arbeitsweise; beurteilt an Hand der Darstellung des Verlaufes und des Ergebnisses evtl. Projekt-/Studienarbeiten sowie der Bachelor-Arbeit	25	
3	Kann ein erfolgreicher Abschluss des Masterstudiums Cyber-Sicherheit erwartet werden: Ursachen, die zum Bachelor-Abschluss mit der Note 3,01-3,49 geführt haben, überzeugende Argumentation seitens des Kandidaten / der Kandidatin, die einen erfolgreichen Abschluss des Masterstudiums erwarten lassen.	25	
4	Grundlegendes Verständnis für aktuelle Forschungsfelder und Entwicklungsrichtungen (aktuelle Fragestellungen) auf dem Gebiet der Cyber-Sicherheit; welches Vertiefungsfeld im Master spricht den/die Studierenden/e besonders an, warum? Passt dieser Studienschwerpunkt zu den Ergebnissen aus dem Bachelorstudium?	25	

Das Qualifizierungsgespräch gilt als bestanden, wenn von der/dem Studierenden mindestens 50% von 100% erreicht wurden.

3. Ergebnis des Qualifizierungsgesprächs:

Ergebnis: ☐ bestanden ☐ nicht bestanden.

 Unterschrift, Datum

 Unterschrift, Datum

 Unterschrift, Datum

 Unterschrift, Datum

 Unterschrift, Datum

¹ Angabe in x % von 100 %

Anlage 3: Verzeichnis verwendeter Abkürzungen

ABaMaPO	Allgemeine Prüfungsordnung für die universitären Bachelor- und Master-Studiengänge der Universität der Bundeswehr München
Abs.	Absatz
Art.	Artikel
Az	Aktenzeichen
BayHIG	Bayerisches Hochschulinnovationsgesetz
bzw.	beziehungsweise
CYB/Ma	Masterstudiengang Cyber-Sicherheit
ECTS	European Credit Transfer and Accumulation System
evtl.	eventuell
FPOCYB/Ma	Fachprüfungsordnung für den universitären Masterstudiengang Cyber-Sicherheit der Universität der Bundeswehr München
HA	Hausarbeit
INF	Informatik
i.V.m.	in Verbindung mit
jew.	jeweils
Matr. Nr.	Matrikelnummer
Max.	Maximal
M.Sc.	Master of Science
mP-xx	mündliche Prüfung mit einer Dauer von xx Minuten
P	Praktikum
Pf	Portfolio
S	Seminar
SemA	Seminararbeit
sP-xx	schriftliche Prüfung mit einer Dauer von xx Minuten
T	Training
TS	Teilnahmeschein
Ü	Übung
UniBw	Universität(en) der Bundeswehr
UniBw M	Universität der Bundeswehr München
V	Vorlesung