



Graduate Programs in Cybersecurity

Master of Professional Studies:
Cybersecurity

Post-Baccalaureate Certificates:
Cybersecurity Operations
Cybersecurity Strategy and Policy
Digital Forensics



CYBERSECURITY - A PROFESSIONALLY-FOCUSED, RELEVANT AND PRACTICAL GRADUATE DEGREE

- » Courses are designed to prepare technical professionals and others in the 'cyber' fields to fill operational management and leadership roles in cybersecurity, cyber operations, and/or related organizations in the government or private sector.
- » Students gain applicable skills that speak to the needs of the operational cybersecurity workforce in Maryland.
- » Cybersecurity is a critical domain of global competition that reaches across social, economic, political and military realms of influence.

WHEN YOU CHOOSE UMBC PROFESSIONAL PROGRAMS, YOU CAN COUNT ON:

- » Classes taught by cybersecurity industry experts with significant current professional experience.
- » Flexible evening, hybrid, online, and/or weekend class schedule that accommodates working professionals.
- » Wide-ranging resources offered at a top-notch public research university.

WHY UMBC?

- » UMBC is uniquely positioned to provide education and training that respond to the state's need for qualified technical professionals in the cybersecurity field.
- » The 2019 U.S. News & World Report Best Colleges guide ranks UMBC in the top ten on its closely-watched Most Innovative Schools list and has recognized UMBC as a global leader in higher education.
- » UMBC is certified as a National Center of Academic Excellence in Cyber Defense Education (CAE/CDE) as well as a Center of Academic Excellence in Cyber Defense Research (CAE-R) sponsored by the National Security Agency and Department of Homeland Security (DHS).
- » UMBC provides a comprehensive and quality education at a manageable cost.

**For program information
in Baltimore:**
Dr. Rick Forno | Program Director
richard.forno@umbc.edu

**For program information
in Rockville:**
Dr. Behnam Shariati
Asst. Program Director
shariati@umbc.edu

For application information:
Baltimore:
Faith Dinh, Program Coordinator
faithdinh@umbc.edu
410-455-6512
Rockville:
Karina Jenkins, Program Manager
sgprofessionalprograms@umbc.edu
301-738-6285

cyber.umbc.edu

ADMISSIONS REQUIREMENTS

M.P.S.

- » A bachelor's degree in Computer Science, Information Systems, or a related field is preferred
- » Minimum undergraduate GPA of 3.0 on a 4.0 scale
- » GRE scores are not required
- » Current professional experience in information technology or cybersecurity

Graduate Certificate

- » A bachelor's degree in any discipline
- » Minimum undergraduate GPA of 3.0 on a 4.0 scale
- » GRE scores are not required for applicants
- » Basic understanding of the internet, networked information systems and information security

INTERNATIONAL APPLICANTS

Please visit cyber.umbc.edu/international for detailed admissions requirements for international applicants.

- » Please pay special attention to English proficiency and testing requirements

ADMISSIONS DEADLINES

Fall: August 1

Spring: December 1

For detailed application process please visit cyber.umbc.edu

*Offered in Baltimore and Rockville.
(schedules may vary)*

Office of Professional Programs

UMBC's Office of Professional Programs offers a broad array of professionally focused master's degree and certificate programs that address industry needs while anticipating future opportunities.

professionalprograms.umbc.edu

Master's of Professional Studies (M.P.S.):

Cybersecurity

30 Credits (10 courses)

REQUIRED CORE COURSES 18 CREDITS

- CYBR 620: Introduction to Cybersecurity
- CYBR 623: Cybersecurity Law & Policy
- CYBR 624: Cybersecurity Project
- CYBR 650: Managing Cyber Operations
- CYBR 652: Enterprise Security
- CYBR 658: Risk Analysis and Compliance

ELECTIVE COURSES SELECT 4 COURSES (12 CREDITS)

- CYBR 621: Cyber Warfare
- CYBR 622: Global Cyber Capabilities and Trends
- CYBR 642: Introduction to Digital Forensics
- CYBR 644: Cyber Practitioner Development Lab **
- CYBR 691: Special Topics in Cybersecurity
- CMPE 685: Principles of Communications Networks *

CERTIFICATE PROGRAMS

POST-BACCALAUREATE CERTIFICATE: CYBERSECURITY STRATEGY & POLICY

REQUIRED COURSES (12 CREDITS)

- CYBR 620: Introduction to Cybersecurity
- CYBR 622: Global Cyber Capabilities and Trends
- CYBR 621: Cyber Warfare
- CYBR 623: Cybersecurity Law & Policy

POST-BACCALAUREATE CERTIFICATE: CYBERSECURITY OPERATIONS

REQUIRED COURSES (12 CREDITS)

- CYBR 620: Introduction to Cybersecurity
- CYBR 650: Managing Cybersecurity Operations
- CYBR 658: Risk Analysis and Compliance
- One Additional Cybersecurity Elective



■ CMSC 644: Information Assurance *

■ CMSC 652: Cryptography and Data Security *

■ CMSC 687: Introduction to Network Security *

■ CMSC 691: Special Topics in Computer Science *

Other relevant graduate course(s) approved by the Cybersecurity Graduate Program Director.

** Offered at Baltimore campus*

*** Pass or fail only. Not a graded course.*

POST-BACCALAUREATE CERTIFICATE: DIGITAL FORENSICS* REQUIRED COURSES (12 CREDITS)

■ CYBR 620: Introduction to Cybersecurity or CMSC equivalent (I.e, CMSC 626, CMSC 687)

■ CYBR 641: Computer Crime Investigations

■ CYBR 642: Introduction to Digital Forensics

■ CYBR 643: Advanced Digital Forensics

** Offered at Baltimore campus only*

All credits earned in these graduate certificates may be applied to the

*Master of Professional Studies (M.P.S.):
Cybersecurity*