

Graduate Programs in CYBERSECURITY



Master's of Professional Studies:
Cybersecurity

Post-Baccalaureate Certificate:
Cybersecurity Operations

Post-Baccalaureate Certificate:
Cybersecurity Strategy and Policy

Post-Baccalaureate Certificate:
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 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, 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 2017 *U.S. News & World Report Best Colleges* guide ranks UMBC in the top five 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 Information Assurance/Cyber Defense Education (CAE-IA/CD) as well as a Center of Academic Excellence in Information Assurance/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.



Offered in
Baltimore:
cyber.umbc.edu

Rockville:
umbc.edu/cybersg

For Program/Academic Information:

Baltimore:
Dr. Rick Forno | Program Director
richard.forno@umbc.edu

Rockville:
Dr. Behnam Shariati | Asst. Program Director
shariati@umbc.edu | 301-738-6019

For Application Information:

Baltimore:
Lisa Gambino | Assistant Director
gambino@umbc.edu | 410-455-3034

Rockville:
sgprofessionalprograms@umbc.edu

Admission 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 for applicants with a degree from an accredited U.S. institution
- » Current professional experience in information technology or cybersecurity

Graduate Certificates:

- » 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 with a degree from an accredited U.S. institution
- » 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

Admission Deadlines

Fall: August 1

Spring: December 1

For detailed application process please visit: cyber.umbc.edu

Offered in Baltimore and Rockville. (schedules may vary)

Master's Program

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

30 Credits (10 courses)

Required 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) 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

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

* Offered at Baltimore campus only | ** Pass or fail only. Not a graded course.



CMPE 685: Principles of Communications Networks *

CMSC 644: Information Assurance *

CMSC 652: Cryptography and Data Security *

CMSC 687: Introduction to Network Security *

CMSC 691: Special Topics in Computer Science *

Certificate Programs

Post-Baccalaureate Certificate: Cybersecurity Strategy & Policy

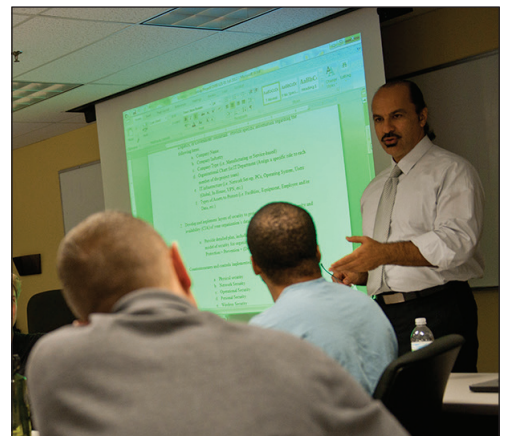
Required Courses (12 Credits)

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 658: Risk Analysis and Compliance

CYBR 650: Managing Cybersecurity Operations

One Additional Cybersecurity Elective

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

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

All credits earned in these graduate certificates may be applied to the Master of Professional Studies (M.P.S.): Cybersecurity

This academic program is a participant in the U.S. Department of Education Gainful Employment program. For more information, <https://gradschool.umbc.edu/resources/careers/gainfulemploy/>