Master of Science Degree
Cybersecurity Technologies

I Year Online, 9 courses, 36 Credits

The Master's Degree in Cybersecurity Technologies is a practical, protocol-driven program designed for professionals who seek expertise in securing digital infrastructure across industries. This 9-course curriculum emphasizes applied security tools, network defense, penetration testing, risk management, incident response, and regulatory compliance. Through hands-on labs, real-world case studies, and simulation-based learning, students will graduate ready to design, implement, and manage effective cybersecurity operations in both public and private sectors. **Courses may be substituted or changed at any time, as curriculums undergo continued revision and updating**.

Foundations of Cybersecurity. Introduction to core cybersecurity principles, terminology, threat types, and defense-in-depth strategies. Includes **Cyber Risk Management and Compliance, r**isk assessment models, governance frameworks, and legal/regulatory standards such as NIST, GDPR, and HIPAA. 4 Credits.

Network Security Protocols. Focus on protocols like SSL/TLS, IPSec, VPNs, and secure email, emphasizing how these protect data in motion. 4 Credits.

Operating System Security. Hardening techniques for Windows, Linux, and macOS systems, covering permissions, audit policies, and system integrity tools. Includes study of secure coding, static/dynamic analysis, and DevSecOps pipeline integration. 4 Credits.

Cyber Threat Intelligence and Analysis. Collecting, analyzing, and acting on threat data to preempt and neutralize cyberattacks. 4 Credits.

Penetration Testing and Ethical Hacking. Hands-on course in vulnerability assessment, red teaming, reconnaissance, and exploitation using industry-standard tools. 4 Credits.

Incident Response and Digital Forensics. Procedures for identifying, containing, eradicating, and recovering from security breaches. Includes evidence collection and chain-of-custody. 4 Credits.

Cryptography and Secure Communications. Covers symmetric/asymmetric encryption, hashing, digital signatures, and secure key management for real-world applications. 4 Credits.

Security Operations Center (SOC) Practices. Structure and workflows of a SOC, including SIEM tools, alert triage, and log analysis in 24/7 environments. Includes **Cloud Security and Virtualization,** namely security challenges and controls in public, private, and hybrid cloud environments, including containers and hypervisors. 4 Credits.

Cloud Security and Virtualization. Security challenges and controls in public, private, and hybrid cloud environments, including containers and hypervisors. 4 Credits.

36 Credits, U.S. Standard for Masters Degree