Master of Science in Applied Cybersecurity and Digital Forensics

At the conclusion of their studies, graduates of the Master of Science in Applied Cybersecurity and Digital Forensics degree should be able to:

- Design and implement a comprehensive enterprise security program using both policy and technology to implement technical, operational and managerial controls.
- Comprehensively investigate information security incidents and violation of law using computer resources in a manner such that all evidence is admissible in a court of law.
- Technically secure enterprise information assets and resources to deter, detect, and prevent the success of attacks and intrusions.
- Conduct and report on significant research in the areas of cybersecurity and/or digital forensics.

Students may choose from two research options to complete the degree:

Thesis Option

The thesis option requires coursework and six credit hours ITMT 591 for a total of 32 credit hours. The result is a master's thesis.

Master's Project Option

The master's project option requires coursework and three credit hours of ITMT 594 or ITMT 597 for a total of 32 credit hours. The result is a project that results in one of the following:

1. A paper submitted for publication as an article or as a technical report
2. A security or forensic software product
3. A security hardware device or appliance

Software or hardware must have an accompanying technical report and user documentation.

Admissions

Applicants for admission to a master of science degree should hold a four-year bachelor's degree in a computing or computing-related engineering discipline from an accredited institution with a minimum cumulative undergraduate GPA of 3.0/4.0 and minimum GRE score of 305 (combined quantitative and verbal), 151 quantitative, and 3.0 analytical writing; international applicants may be required to submit a TOEFL score. Applicants admitted to a master of science degree who do not hold a four-year bachelor's degree in a computing or computing-related engineering discipline may be required to complete up to one year of prerequisite courses prior to beginning formal graduate studies.

Current prerequisites for the Master of Science in Applied Cybersecurity and Digital Forensics include computer hardware and operating system literacy (ITM 301 or equivalent coursework, certification, or experience); an ability to program at a competent level using a contemporary programming language (ITMD 411 or ITMD 510); basic knowledge of networking concepts, protocols, methods, and the Internet (ITMO 440 or ITMO 540); the ability to create and administer databases using a modern database management system (ITMD 421); and completion of a program of mathematics culminating in a calculus-based course in probability and statistics (MATH 474).

Degree Requirements

Required Core Courses (15 credit hours)		
ITMS 538	Cyber Forensics	3
ITMS 543	Vulnerability Analysis and Ctrl	3
ITMS 548	Cyber Security Technologies	3
ITMS 578	Cyber Security Management	3
LAW 273	Evidence	3
Research Courses (6-8 credit hours)		
ITMT 591	Research (Thesis)	6-8
or for the project track		6
	ITMS 539 Steganography	3
	or ITMS 549 CST: Projects & Adv Methods and	
	ITMT 594 Special Projects in IT	3
	or ITMT 597 Special Problem in IT	
Elective Courses (9-11 credit hours)		
Select seven to nine credit hours from the following:		7-9
Any 500-level ITMS course not listed in the required courses above.		3
ITMM 585	Lgl&Ethical Issues in Info Tech	3
ITMM 586	IT Auditing	3
ITMO 556	Intro to Open Source Software	3
ITMT 597	Special Problem in IT	3
Select a minimum of two credit hours from the following:		2
LAW 240	National Security Law	2
LAW 495	Electronic Discovery	2
Minimum degree credits required:		**32**

Perlstein Hall Suite 223 | 10 West 33rd Street | Chicago, Illinois 60616 | 312.567.5290 | appliedtech.iit.edu/itm