**بسم الله الرحمن الرحيم**

# الجامعــة الهاشميــة

## كلية الأمير الحسين بن عبدالله الثاني لتكنولوجيا المعلومات

## قسم أنظمة المعلومات الحاسوبية

**ماجستير في الامن السيبراني**

**(مسار الرسالة)**

**خطة عام 2019**

**بسم الله الرحمن الرحيم**

**الجامعة الهاشمية**

**كلية الامير الحسين بن عبدالله الثاني لتكنولوجيا المعلومات**

**متطلبات الحصول على درجة الماجستير في الامن السبيراني**

**البرنامج الدراسي: ماجستير : ماجستير في الامن السبيراني**

**نوع الخطـــة: مسار الرسالة**

**السنة الدراسية: 2019**

**أولاً: أحكام وشروط عامة**

- **تلتزم هذه الخطة بالإطار العام لبرنامج الماجستير في الجامعة الهاشمية.**
- **يقبل في هذا البرنامج الطلبة الحاصـــلون على درجة البكالوريوس في تخصـــصـــات تكنولوجيا المعلومات.**

**ثانياً: تتكون الخطة الدراسية من (33) ثلاث وثلاثين ساعة معتمدة موزعة على النحو التالي:**

**عدد الساعات المعتمدة**

| | |
|---|---|
| **متطلبات التخصص :** | **24** |
| **أ- إجبارية** | **15** |
| **ب- اختيارية** | **9** |
| **رسالة** | **9** |
| **المجموع** | **33** |

**متطلبات التخصص** **الساعات المعتمدة: ٢٤**

**نوع المتطلب: اجبارية** **الساعات المعتمدة: ١٥**

| رقم المادة | اسم المادة | الساعات المعتمدة | نظري | عملي | المتطلب السابق |
|---|---|---|---|---|---|
| 1910021711 | أمن المعلومات | 3 | 3 | 0 | - |
| 1910021730 | التحقيق الرقمي | 3 | 3 | 0 | - |
| 1910021731 | القرصنة الأخلاقية | 3 | 3 | 0 | - |
| 1910021742 | مراقبة أنظمة الدفاع السيبراني | 3 | 3 | 0 | - |
| 1910021792 | منهجية البحث العلمي | 3 | 3 | 0 | - |

**متطلبات التخصص** **الساعات المعتمدة: 24**

**نوع المتطلب: اختياري** **الساعات المعتمدة: 9**

| رقم المادة | اسم المادة | الساعات المعتمدة | نظري | عملي | المتطلب السابق |
|---|---|---|---|---|---|
| 1910021743 | ادارة مخاطر الأمن السيبراني | 3 | 3 | 0 | - |
| 1910021712 | أمن الشبكات اللاسلكية والأنظمة المحمولة | 3 | 3 | 0 | - |
| 1910021732 | طرق القرصنة | 3 | 3 | 0 | - |
| 1910021733 | فحص الاختراق | 3 | 3 | 0 | - |
| 1910021794 | مواضيع خاصة في الامن السيبراني | 3 | 3 | 0 | - |
| 1910021734 | علم التشفير | 3 | 3 | 0 | - |
| 1910021744 | إدارة الكوارث والأزمات | 3 | 3 | 0 | - |
| 1910021741 | ادارة وتحليل البيانات الضخمه | 3 | 3 | 0 | - |
| 1910021761 | التجاره والتسويق الالكتروني | 3 | 3 | 0 | - |
| 1910021782 | تكنولوجيا الويب | 3 | 3 | 0 | - |

**الرسالة ورقمها : 1910021799 الساعات المعتمدة : 9**

# المواد التي تطرح من قسم أنظمة المعلومات الحاسوبية

| رمز المساق ورقمه | اسم المساق | الساعات المعتمدة | الساعات الاسبوعية | | المتطلب السابق |
|---|---|---|---|---|---|
| | | | نظري | عملي | |
| 1910021711 | أمن المعلومات | 3 | 3 | 0 | – |
| 1910021730 | التحقيق الرقمي | 3 | 3 | 0 | – |
| 1910021731 | القرصنة الأخلاقية | 3 | 3 | 0 | – |
| 1910021742 | مراقبة انظمة الدفاع السيبراني | 3 | 3 | 0 | – |
| 1910021792 | منهجية البحث العلمي | 3 | 3 | 0 | – |
| 1910021732 | طرق القرصنة | 3 | 3 | 0 | – |
| 1910021733 | فحص الاختراق | 3 | 3 | 0 | – |
| 1910021794 | مواضيع خاصة في الامن السيبراني | 3 | 3 | 0 | – |
| 1910021795 | الامتحان الشامل | 0 | 0 | 0 | – |
| 1910021743 | ادارة مخاطر الأمن السيبراني | 3 | 3 | 0 | – |
| 1910021712 | أمن الشبكات اللاسلكية والأنظمة المحمولة | 3 | 3 | 0 | – |
| 1910021734 | علم التشفير | 3 | 3 | 0 | – |
| 1910021744 | إدارة الكوارث والأزمات | 9 | 9 | 0 | – |
| 1210021741 | ادارة وتحليل البيانات الضخمه | 3 | 3 | 0 | – |
| 1210021761 | التجاره والتسويق الالكتروني | 3 | 3 | 0 | – |
| 1910021782 | تكنولوجيا الويب | 3 | 3 | 0 | – |

# The Hashemite University

## Prince Al-Hussein Bin Abdullah II Faculty for Information Technology
## Department of Computer Information Systems
## Master in Cyber Security
## (Thesis Track)
## Study Plan 2019

**A. Compulsory Courses (15 hours)**

| Course Number | Course | Credit Hours | Theory | Practical | Prerequisite |
|---|---|---|---|---|---|
| 1910021711 | Information security | 3 | 3 | 0 | – |
| 1910021730 | Digital Forensics | 3 | 3 | 0 | – |
| 1910021731 | Ethical Hacking | 3 | 3 | 0 | – |
| 1910021742 | Cyber Defense Monitoring | 3 | 3 | 0 | – |
| 1910021792 | Research Methodology | 3 | 3 | 0 | – |

**B. Elective Courses (9 hours)**

| Course Number | Course | Credit Hours | Theory | Practical | Prerequisite |
|---|---|---|---|---|---|
| 1910021743 | Cyber Security Risk Management | 3 | 3 | 0 | – |
| 1910021712 | Wireless Network and Mobile Systems Security | 3 | 3 | 0 | – |
| 1910021732 | Hacking Techniques | 3 | 3 | 0 | - |
| 1910021733 | Penetrating Testing | 3 | 3 | 0 | - |
| 1910021794 | Special topics in Cyber Security | 3 | 3 | 0 | - |
| 1910021734 | Cryptography | 3 | 3 | 0 | - |
| 1910021744 | Disaster and Crises Management | 3 | 3 | 0 | - |
| 1910021741 | Big Data Analytic and Management | 3 | 3 | 0 | - |
| 1910021761 | e-Commerce and e-Marketing | 3 | 3 | 0 | - |
| 1910021782 | Web technology | 3 | 3 | 0 | - |

**C. Thesis – 1910021799- (9 hours)**

# Courses' Description

## 1. Information Security:

Information Security is a comprehensive study of the principles and practices of computer system security including operating system security, network security, software security and web security. Topics include common attacking techniques such as virus, trojan, worms and memory exploits; the formalisms of information security such as the access control and information flow theory; the common security policies such as BLP and Biba model; the basic cryptography, RSA, cryptographic hash function, and password system. The real system implementations, with case study of UNIX, SE-Linux, and Windows; network intrusion detection; software security theory; web security; legal and ethical issues in computer security.

## 2. Digital Forensics

This course presents an overview of the principles and practices of digital investigation. The objective of this class is to emphasize the fundamentals and importance of digital forensics. Students will learn different techniques and procedures that enable them to perform a digital investigation. This course focuses mainly on the analysis of physical storage media and volume analysis. It covers the major phases of digital investigation such as preservation, analysis. This course will provide theoretical and practical knowledge, as well as current research on Digital Forensics. Upon completion of the course, students can apply open-source forensics tools to perform digital investigation and understand the underlying theory behind these tools.

## 3. Ethical Hacking

Introduction to the principles and techniques associated with the cybersecurity practice known as ethical hacking. The course covers planning, reconnaissance, scanning, exploitation, post-exploitation, and result reporting. The student discovers how system vulnerabilities can be exploited and learns to avoid such problems. The course will provide the fundamental information associated with each of the methods employed and insecurities identified. In all cases, remedial techniques will be explored. Students will develop an excellent understanding of current cybersecurity issues and ways that user, administrator, and programmer errors can lead to exploitable insecurities.

**4. Cyber Defense Monitoring:**

This course concentrates on a number of important Cyber Defense Monitoring techniques and solutions. The course focuses on event logging and collection with syslog protocol, regular expression language and its applications to system/network monitoring, event correlation, and finally network intrusion detection and prevention. The course also discusses a number of open-source monitoring solutions, including UNIX rsyslog package, Simple Event Correlator, and Snort IDS/IPS.

**5. Research Methodology:**

This course has a vocational focus. It assists students to develop skills in research and scientific communication in the relevant discipline. Topics addressed include design and performance of experiments or action research, analysis and presentation of research data, and preparation of oral and written scientific reports that use these skills. The aim of the course is to prepare students to apply research focused on one of the following:

- Hacking techniques.
- Digital forensics.
- Security protocols.
- Monitoring the cyberspace.

**6. Cyber security Risk Management:**

As organizations are vulnerable to different types of cyberattacks, and due to the limitations in organizational resources, the ability to perform risk management has become crucial for organizations to defend their system. This course will help students identify and analyze information security vulnerabilities and threats in their organizations. Students also will be able to develop risk mitigation strategies to respond to different types of cyberattacks including the appropriate legal and compliance steps that need to be undertaken.

**7. Wireless network and mobile systems security**

The course is an advanced course of security in mobile communication systems, including mobile/cellular telephony, wireless Internet, mobile ad hoc, IoT systems and sensor networks. The course covers protocols and configurations for realizing authentication, key distribution, integrity, confidentiality and anonymity in wireless networks. The course introduces an overview of security principles in several generations of mobile networks, from GSM (2G), UMTS (3G) up until LTE (4G). Security models of popular mobile device platforms are also introduced including IOS,

Android and the Windows Phone. Security in mobile services, such as VoIP, text messaging, WAP and mobile HTML are also introduced.

**8. Hacking Techniques:**

This course helps students understand malicious, black hat attackers' tactics and strategies in detail. The course also teaches students how to use the same hacking techniques to perform a white-hat, ethical hack, on their organization. It teaches students how hackers undermine systems and how to prepare, detect, and respond to computer incidents. The course covers fundamentals of hacking, the latest information and strategies in penetration testing, footprinting, vulnerability scanning and exploits, and network traffic analysis.

**9. Special topics in cyber security:**

Topics will be assigned by the department on evolving techniques and related topics to support the study plan and to encourage further research by students.

**10. Dissertation:**

Each student must complete, document, present and defend a thesis under the supervision of a faculty member in the fields of Information Systems Security and cyber security. Every candidate must complete a thesis (equivalent to 9 credit hours) describing research work of publishable quality. The thesis must be defended before a committee consisting of the supervisor and at least three other faculty members, one from outside the university, in the relevant fields. The thesis defense is open to all interested faculty and students. Upon the completion of 15 credits, a student is eligible to register for thesis.

**11. Penetration Testing**

This course enhances the business skills needed to identify protection opportunities and optimize security controls in an organization. In this course, students will learn how to use ethical hacking to discover weakness in their organization and how to gather intelligence by employing reconnaissance, published data, and scanning tools. In this course, students will go through a complete penetration test and create assessment reports using latest tools such as Saint, Metasploit through Kali Linux and Microsoft PowerShell.

**12. Cryptography:**

This course will cover the cryptography and crypto-analysis techniques. It will introduce the symmetric and asymmetric encryption, private and public key encryption, key distribution, cryptographic hash functions stream ciphers, zero-knowledge proof systems, cryptanalytic attacks and brute-force attacks.

**13. Disaster and Crises Management**

This course covers topics related to disaster recovery and emergency planning and management as applied to the information-systems function in corporations. Topics include security risk evaluation and management, creation of threat profiles, continuity of operations planning, contingency planning, and incident reporting. A self-directed approach/tool for the conduct of information security risk evaluation is introduced. Projects include developing a security protection strategy and plan.

**14. Web Technology**

Web Technology: this course introduces World Wide Web Consortium (W3C) standard markup language and services of the Internet. It introduces the creation of web graphics using web graphics file types, optimization, RGB color, web typography, elementary special effects, transparency, animation, slicing, basic photo manipulation, and other related topics. In addition, it introduces W3C standard client-side Internet programming using developed programming languages. Finally, it includes the creation of web sites and applets using web development software. This course also gives an introduction to web intelligence (WI). WI is a combination of digital analytics, which examines how website visitors view and interact with a site's pages and features, and business intelligence, which allows a corporation's management to use data on customer purchasing patterns, demographics, and demand trends to make effective strategic decisions.

**15. Big Data Analytics and Management**

This course is an introduction to the concepts of "Big Data" and "data analysis". It provides an introduction to one of the most common frameworks, Hadoop, that has made big data analysis easier and more accessible. At the end of this course, students are expected to first, describe the Big Data landscape including examples of real-world big data problems including the three key sources of Big Data: people, organizations, and sensors. Second, explain the V's of Big Data (volume, velocity, variety, veracity, valence, and value) and why each impacts data collection, monitoring, storage, analysis, and reporting. Third, to have some Practical experience with some commonly used tools and techniques for (big) data processing. Forth, know the basics of distributed file systems, databases, and computing. Fifth, to have gained practical data processing skills with the MapReduce framework / Apache Hadoop.

**16. Comprehensive Exam**

The student has to sit for the comprehensive exam in a semester in which he/she has not registered any other course and after he has completed all the program requirements. The exam will be in a number of compulsory courses that have been chosen by the department council.

17. **e-Commerce and e-Marketing**

e-Commerce and e-Marketing :This course examines the advanced concepts, technology, and applications of electronic commerce, or e-commerce. Since users can engage in e-commerce from a fixed device (e.g., PC) or from a mobile device (e.g., mobile phone) we will examine both traditional fixed e-commerce and mobile e-commerce or m-commerce. The course begins by setting the context for ecommerce within the domain of information systems. It examines security and payment in e-commerce. It explains the technological infrastructure needed to support an e-commerce system and describes how e-commerce systems are built. Next the course examines m-commerce in detail. It presents m-commerce concepts and discusses the technology needed for m-commerce. It examines the range of commerce applications and discusses mobile security and payment. The course concludes with a presentation on the future of e-commerce. The focus is on analytical skills during electronic businesses applications.