عنوان الماستر: اقتصاد رقمى
السداسي: الثالث
اسم الوحدة: إستكشافية
اسم المادة: الأمن السيبرانى
الرصيد: 2
المعامل: 2
نمط التعليم: حضورى

أهداف التعليم: الأهداف العامة التي يمكن تحقيقها من خلال تدريس الأمن السيبراني:

- فهم مفاهيم وقضايا الأمن السيبراني.
- تحديد أنواع هجمات الكمبيوتر ونقاط ضعف أنظمة المعلومات.
- التعرف على تقنيات الأمن السيبراني وآليات الدفاع وكيفية عملها.
- تعرف على كيفية وضع السياسات الأمنية وإجراءات الاستجابة للحوادث الأمنية.
- فهم المعايير و الجوانب القانونية للأمن السيبراني والآثار القانونية للحوادث الأمنية والالتزامات لذلك.
- تتوفر لطالب القدرة على تحليل المخاطر الأمنية وتنفيذ إجراءات الوقاية والحماية.
- التعرف على أفضل الممارسات في الأمن السيبراني لحماية البيانات وأنظمة المعلومات.

المعارف المسبقة المطلوبة :
المتطلبات العامة التي يجب أخذها في الاعتبار:

- تكنولوجيا المعلومات والاتصال.
- المعرفة الأساسية بالكمبيوتر (المعرفة الأساسية بأنظمة تشغيل الكمبيوتر والشبكات والتطبيقات).
- مهارات البرمجة (المعرفة في البرمجة خاصة في لغات البرمجة النصية مثل Python أو Perl أو Ruby).
- دراية لقواعد أمان الكمبيوتر (هجمات رفض الخدمة وفيروسات الكمبيوتر والبرامج الضارة).
- مهارات في الرياضيات (فهم مفاهيم التشفير و الرياضيات لا سيما نظرية الأرقام و المنطق).

محتوى المادة:

- **المحور الأول:** مقدمة في الأمن السيبراني: المفاهيم والتعاريف الأساسية و قضايا الأمن السيبراني في المجتمع الحديث.
- **المحور الثانى:** أنواع هجمات الكمبيوتر: الفيروسات والبرامج الضارة (malwares) والتصيد الاحتيالي (phishing) وبرامج الفدية (ransomwares).

- **المحور الثالث:** تقنيات الأمن السيبراني: جدار الحماية ، مكافحة الفيروسات، مكافحة البريد العشوائي، والتشفير، المصادقة، إدارة الهوية والوصول (أنظمة المصادقة سياسات الوصول، ضوابط الأمن).
- **المحور الرابع:** معايير ولوائح الأمن السيبراني: GDPR، PCI DSS، ISO 27001، إلخ، أفضل ممارسات الأمن السيبراني: السياسات الأمنية، إجراءات الاستجابة للحوادث، وعي المستخدم ، إلخ.
- **المحور الخامس:** تقنيات التحقيق في الأمن السيبراني: جمع الأدلة، تحليل السجلات ، التحقيقات الرقمية و الاتجاهات الناشئة في الأمن السيبراني: الذكاء الاصطناعي، إنترنت الأشياء، التهديدات المستمرة المتقدمة.
- **المحور السادس:** أمان الشبكة: بروتوكولات الاتصال الآمنة، وآليات الدفاع ضد هجمات رفض الخدمة الموزعة (DDoS) ، وبنى الشبكات الآمنة، أمان نظام التشغيل (نقاط الضعف الشائعة في نظام التشغيل، وآليات حماية الذاكرة، لمحاكاة الافتراضية)، أمان التطبيق (ثغرات تطبيق الويب وتقنيات إدخال التعليمات البرمجية، بروتوكولات أمان التطبيقات)، أمان السحابة (تحديات أمان السحابة، آليات التحكم في الوصول، هوية السحابة وإدارة الوصول)، أمان الكائنات المتصلة (نقاط الضعف في الكائنات المتصلة، بروتوكولات الاتصال الآمنة للكائنات المتصلة، إدارة الهوية والوصول للكائنات المتصلة)، الأمن السيبراني الهجومي (تقنيات القرصنة الأخلاقية، اختبار الاختراق، تقنيات الهجوم المتقدمة).
- **المحور السادس:** الجوانب القانونية للأمن السيبراني: المسؤولية القانونية في حالة وقوع حادث أمني، التزامات الإخطار، العقوبات الجنائية.
- **المحور السابع:** دراسات حالة الأمن السيبراني: أمثلة ملموسة للحوادث الأمنية والحلول الموضوعة لمعالجتها.

طريقة التقييم: تقييم مستمر + امتحان نهائي ويقاس معدل المادة بالوزن الترجيحي للدروس (60%) والأعمال الموجهة (40%)

المراجع:

- ✓ الجبرين، عمر. (2017). الأمن السيبراني وحماية المعلومات. الرياض: دار اليمامة.
- ✓ الشوبكي، عبد الحميد. (2018). أمن الإنترنت والتواصل الآمن. بيروت: دار المشرق.
- ✓ الحمادي، سالم، والنقبي، عبد الله. (2015). السيبرانيات: المفاهيم والتقنيات والتحديات. أبوظبي: هيئة الإمارات للمعرفة الحكومية.
- ✓ المنصوري، حاتم. (2016). الأمن السيبراني والتحديات الراهنة. دبي: دار المؤرخ العربي.
- ✓ الصفار، مصطفى. (2016). السيبرانيات والأمن السيبراني. الرياض: العالم العربي.
- ✓ الحمداني، علي. (2014). أمن المعلومات والسيبرانيات. بغداد: دار العرب للنشر.
- ✓ الحياري، يوسف. (2019). الأمن السيبراني: المفاهيم والتطبيقات. عمان: دار الفارابي.

- ✓ الحموري، خالد، والحموري، عبد الله. (2017). أمن المعلومات والسيبرانية: الحماية الشاملة للمنظمات. عمان: دار وائل للنشر والتوزيع.
- ✓ الشريدة، محمد، والخطيب، رائد. (2016). السيبرانية وأمن المعلومات: الدليل العملي لتأمين شبكات الحاسوب. عمان: دار عالم الفوائد للنشر والتوزيع
- ✓ Avoine, G., Deltel, J.-M., Gillet, P., & Lemaire, V. (2019). Cybersécurité : comprendre, prévenir, agir. Dunod.
- ✓ Lardy, J.-P. (2015). Sécurité informatique : principes et méthodes. Dunod.
- ✓ Archimbaud, J.-L., & Jolion, J.-M. (2018). Les fondamentaux de la sécurité de l'information. Dunod.
- ✓ Tissier, G. (2019). Gestion de la sécurité de l'information : ISO 27001 et risques informatiques. Dunod.
- ✓ Fournier, C., & Godart, C. (2018). Cybersécurité : guide pratique pour les managers. Dunod.
- ✓ Msahli, M. (2019). Cybersécurité : menaces, vulnérabilités et contrôles. Dunod.
- ✓ Gobry, P.-E., & Harrel, Y. (2018). Cybersécurité et gouvernance des systèmes d'information. Éditions ENI.
- ✓ Mattatia, F. (2018). Cybersécurité : 100 fiches pratiques pour préserver votre identité numérique. Dunod.
- ✓ Schwarz, G. (2020). La cybersécurité en France. Robert Laffont.
- ✓ Freyssinet, E., & Rigaux, P. (2018). Cybermenaces : la guerre est déclarée. Eyrolles.
- ✓ Pierrat, L., & Bahloul, K. (2018). Cyber-résilience : sécurité informatique et continuité d'activité. Dunod.