

السداسي: الثالث
وحدة التعليم: وحدة التعليم المنهجية
المادة: الأمن السيبراني
الرصيد: 05
المعامل: 02
نمط التعليم: حضوري

أهداف التعليم :-

1. فهم مفاهيم الأمن السيبراني: يجب على الطلاب فهم مفاهيم الأمن السيبراني مثل الهجمات السيبرانية والتهديدات والاختراقات الإلكترونية وتقنيات الحماية المختلفة.
 2. تطوير مهارات الحماية: يجب على الطلاب تعلم مهارات الحماية والتدابير الوقائية التي يمكن اتخاذها لتأمين البيانات والشبكات والأجهزة الإلكترونية.
 3. استخدام التقنيات الحديثة: يجب على الطلاب تعلم استخدام التقنيات الحديثة المستخدمة في مجال الأمن السيبراني مثل تقنيات التشفير والأمان الإلكتروني والواقع الافتراضي والذكاء الاصطناعي.
 4. تعزيز الوعي الأمني: يجب على الطلاب تعزيز الوعي الأمني لدى الأفراد والمؤسسات والحكومات وفهم أهمية الأمن السيبراني
- المعارف المسبقة المطلوبة:**
مهارات التعامل مع الانترنت

محتوى المادة:

- المحور الأول:** مفاهيم الأمن السيبراني في المالية الإلكترونية: يمكن تعريف مفاهيم الأمن السيبراني وتطبيقها على مجال التكنولوجيا المالية، مثل الهجمات الإلكترونية وطرق الوقاية منها.
- المحور الثاني:** حماية البيانات المالية: يمكن الحديث عن طرق حماية البيانات المالية والتأكد من سريتها وأمانها، بما في ذلك تقنيات التشفير وإجراءات الحماية الأخرى.
- المحور الثالث:** حماية البيانات المالية: يمكن الحديث عن طرق حماية البيانات المالية والتأكد من سريتها وأمانها، بما في ذلك تقنيات التشفير وإجراءات الحماية الأخرى.
- المحور الرابع:** التدريب على الأمن السيبراني: يمكن الحديث عن أهمية تدريب الموظفين على الأمن السيبراني والوقاية من الهجمات الإلكترونية في مجال التكنولوجيا المالية.
- المحور الخامس:** إدارة الحوادث الأمنية: يمكن الحديث عن كيفية إدارة الحوادث الأمنية والاستجابة لها في حالة حدوثها، بما في ذلك إجراءات الطوارئ والتقارير المطلوبة.
- المحور السادس:** الأمن السيبراني في التحويلات المالية: يمكن الحديث عن أمن التحويلات المالية وكيفية حمايتها من الاختراق والاحتيال.
- المحور السابع:** القوانين واللوائح المتعلقة بالأمن السيبراني في المالية: يمكن الحديث عن القوانين واللوائح المتعلقة بالأمن السيبراني في المالية وكيفية الامتثال لها

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

المراجع:

- المجلس الأعلى لتنظيم الاتصالات. (2019). الدليل الوطني لأمن المعلومات. المملكة العربية السعودية.
- الجامعة العربية. (2017). الأمن السيبراني في الوطن العربي: التحديات والفرص. مصر.
- مؤسسة الأمير سلطان بن عبدالعزيز العالمية للإعلام الإلكتروني. (2019). الأمن السيبراني وتحدياته في العالم العربي. المملكة العربية السعودية.
- McAfee, Inc. (2018). Economic Impact of Cybercrime— No Slowing Down. United States.
- NIST Special Publication 800-53. (2020). Security and Privacy Controls for Information Systems and Organizations. United States.
- World Economic Forum. (2019). Global Risks Report 2019. Switzerland