



ماجستير العلوم في حوسبة الجيل القادم

المسار: الذكاء الاصطناعي والأساليب الشكلية للأمن السيبراني
عدد الساعات المعتمدة للمسار: 36

1. نظرة عامة على البرنامج

مع تزايد حجم الهجمات الإلكترونية وتعقيدها، أصبح من الضروري استخدام أساليب جديدة للحفاظ على نفس مستوى الأمان. ومن بين هذه الأساليب استخدام الذكاء الاصطناعي لتزويد محلي عمليات الأمن السيبراني بالقدرة على الكشف المبكر عن التهديدات الأمنية ونقاط الضعف. ومن الأساليب الجديدة الأخرى استخدام تقنيات الأساليب الشكلية للتحقق من عدم وجود نقاط ضعف أمنية في مرحلة التصميم، مما يسمح بإنشاء بروتوكولات وأنظمة حيوية عالية الأمان. يجمع هذا البرنامج بين الذكاء الاصطناعي والأساليب الرسمية لتطوير الجيل القادم من حلول الأمن السيبراني، بما يتيح فرصاً بحثية وتطبيقية واعدة، ويسهم في تعزيز الابتكار في هذا المجال الحيوي.

للحصول على درجة الماجستير، يجب على الطلاب إكمال 36 ساعة معتمدة على النحو التالي:

2. خطة الدراسة

رمز المقرر	عنوان المقرر	الساعات المعتمدة
الفصل الدراسي الأول		
NGCM601	المنطق والرياضيات المتقطعة	2
NGCM602	أسس علوم الحاسوب	2
NGCM603	أساسيات الذكاء الاصطناعي	2
NGCM604	البرمجة كائنية التوجه وتحليل البيانات	2
NGCM605	الكتابة العلمية	1
إجمالي الساعات المعتمدة		9
الفصل الدراسي الثاني		
NGCM611	أساسيات الأمن السيبراني	2
NGCM612	الذكاء الاصطناعي لأمن المعلومات	2
NGCM613	الأساليب الشكلية لأمن المعلومات	2
NGCM614	الحوسبة الكمية والأمن السيبراني	2
NGCM615	منهجية البحث	1
إجمالي الساعات المعتمدة		9



رمز المقرر	عنوان المقرر	الساعات المعتمدة
الفصل الدراسي الثالث		
انظر قائمة المقررات الاختيارية	2 مقررات اختيارية	4
NGCM697	مواضيع متقدمة ومتخصصة في الأمن السيبراني	1
NGCM698	مشروع تطبيقي	4
إجمالي الساعات المعتمدة		9
الفصل الدراسي الرابع		
NGCM699	رسالة الماجستير	9
إجمالي الساعات المعتمدة		9
إجمالي الساعات المعتمدة للبرنامج		36

المقررات الاختيارية:

رمز المقرر	عنوان المقرر	الساعات المعتمدة
NGCM 641	القرصنة الأخلاقية والدفاع عن الأنظمة	2
NGCM 642	أمن الشبكات والتطبيقات	2
NGCM 643	أمن التقنيات الناشئة	2
NGCM 644	إدارة المخاطر السيبرانية	2
NGCM 645	التحليل الجنائي الرقمي	2
NGCM 646	البيانات الضخمة والذكاء الاصطناعي المتقدم	2



3. وصف المقررات

المنطق والرياضيات المتقطعة (NGCM601)

في هذا المقرر، سنقدم المفاهيم الأساسية للمنطق ونناقش ما يجعل بعض الحجج صحيحة أو غير صحيحة. ويؤدي ذلك إلى تعريف الإثبات الرياضي، ولا سيما الاستقراء الرياضي. يركز هذا المقرر على المفاهيم المتقدمة للمنطق، ونظرية الأنواع، ونظرية الرسوم البيانية.

أسس علوم الحاسوب (NGCM602)

في هذا المقرر، يتعرف الطلاب على بنية الحاسوب وبرامج النظام (المصروفات، والمجمّعات، والمحملات، وأنظمة التشغيل). وتتم مناقشة كل من المفاهيم الأساسية والأمثلة العملية. بعد ذلك، سنقدم مقدمة عن الخوارزميات وهياكل البيانات. ويهدف المقرر إلى تزويد الطلاب بمجموعة من الخوارزميات والهياكل الأساسية، بالإضافة إلى المهارات اللازمة لتحليل تعقيد الخوارزميات وإثبات صحتها.

أساسيات الذكاء الاصطناعي (NGCM603)

في هذا المقرر، سنقدم مبادئ الذكاء الاصطناعي وتطبيقاته وحالات استخدامه، وكيف يغير حياتنا. سنقدم موضوعات أساسية في الذكاء الاصطناعي مثل حل المشكلات، وتمثيل المعرفة والاستدلال، واتخاذ القرار في ظل عدم اليقين. بعد ذلك، سنستكشف أساسيات التعلم الآلي والتعلم العميق وأكثر خوارزميات التعلم شيوعاً، بما في ذلك تقنيات التعلم الآلي التعزيزي الخاضعة للإشراف وغير الخاضعة للإشراف وشبه الخاضعة للإشراف.

البرمجة كائنية التوجه وتحليل البيانات (NGCM604)

تقدم البرمجة كائنية التوجه العديد من المزايا، بما في ذلك التطوير السريع وإمكانية إعادة الاستخدام وتقليل تكاليف الصيانة. تم تصميم هذا المقرر لتعزيز مهارات البرمجة لدى الطلاب من خلال مشاريع شاملة. وهي تغطي المبادئ الأساسية للبرمجة كائنية التوجه وتوفر تعرضاً واسعاً لمجالات البرمجة مثل التطبيقات متعددة الخيوط والتواصل بين العمليات وتفاعلات قواعد البيانات. بالإضافة إلى ذلك، سنركز على أدوات تصوير البيانات وتعليم الطلاب كيفية استخلاص الاستنتاجات من البيانات. سيتعلم الطلاب كيفية تصوير البيانات بصرياً، وتحليل اتجاهات البيانات، وإنشاء لوحات معلومات تفاعلية.

الكتابة العلمية (NGCM 605)

يقدم هذا المقرر المكونات الأساسية للكتابة العلمية الفعالة، مع التركيز على صياغة الأوراق البحثية للنشر. من خلال الدروس التفاعلية والتمارين العملية، سيتعلم المشاركون كيفية تنظيم مخطوطة بحثية، وتطبيق مبادئ الكتابة العلمية، والتعرف على عملية النشر.

أساسيات الأمن السيبراني (NGCM611)

تتضمن بعض الهجمات الأكثر تدميراً على أنظمة الحاسوب اليوم استغلال البنية التحتية للشبكة، إما كهدف للهجوم أو كوسيلة لمهاجمة الأنظمة النهائية. يركز هذا المقرر على أساسيات أمن الشبكات ويقدم دراسة متعمقة لتقنيات الهجوم على الشبكات وطرق الدفاع ضدها. ثم يعرض المقرر المتطلبات والقدرات الأمنية المتوقعة من الأجهزة الحديثة وأنظمة التشغيل وبيئات البرامج الأخرى. سنقدم موضوعات مثل أمن الأجهزة، وأمن x86، والقنوات الجانبية، وأمن OS، وأمن Windows وLinux، وSELinux، وأمن Android، وبيئات التنفيذ الموثوقة، وبرامج المراقبة الافتراضية، وتحصين النظام. وأخيراً، سنقدم أساسيات وتطبيقات التشفير. وسنركز على الأدوات الرئيسية للتشفير الحديث: التشفير المتماثل والمصادقة، وتشفير المفتاح العام، واتفاق المفتاح، وأنظمة التوقيع الرقمي، و بعض تقنيات تحليل الشفرات.

الذكاء الاصطناعي لأمن المعلومات (NGCM612)

الهدف من هذا المقرر هو شرح كيفية تطبيق التعلم الآلي على الأمن السيبراني الحديث وكشف التهديدات. سنقدم الأدوات والتقنيات المستخدمة في التخفيف من تهديدات الشبكات وتطبيقات البرمجيات، وسنشرح كيفية استخدام الذكاء الاصطناعي لدعم محلي الأمن في عملهم.

الأساليب الشكلية لأمن المعلومات (NGCM613)



يهدف هذا المقرر إلى شرح كيفية استخدام المنطق لنمذجة المشكلات ذات الطبيعة الحسابية أو الرياضية وكيفية استخدام أجهزة الحاسوب لتحقيق ذلك. على وجه الخصوص، سنقدم أدوات مساعدة الإثبات، التي تسمح للمرء بتقنين التفكير البشري من خلال بناء البراهين بشكل تفاعلي وشرح استخدامها للتأكد من عدم وجود أخطاء في البرامج. بعد ذلك، سنركز على نمذجة وتحليل بروتوكولات الأمان للأنظمة الحيوية باستخدام الأساليب الرسمية، بدءاً من بروتوكولات المصادقة لأمن الشبكات وصولاً إلى بروتوكولات التصويت الإلكتروني والخدمات المصرفية عبر الإنترنت. سنقدم الأفكار الرئيسية والأسس النظرية للنمذجة الرسمية وتحليل بروتوكولات الأمان باستخدام أحدث الأدوات.

الحوسبة الكمّية والأمن السيبراني (NGCM614)

يقدم هذا المقرر أساسيات الحوسبة الكمّية (البت الكمّي والدوائر الكمومية والتشابك الكمّي) ويحلل تأثيرها على الأمن السيبراني. يدرس الطلاب الخوارزميات الكمّية مثل خوارزميات شور وغروفر التي تهدد أنظمة التشفير الحالية، ويستكشفون الحلول المقاومة للحوسبة الكمّية، بما في ذلك تشفير ما بعد الكم (مثل Kyber و Dilithium) وتوزيع المفاتيح الكمومية (QKD). يُعد المقرر الطلاب للانتقال إلى عصر الحوسبة الكمّية.

منهجية البحث (NGCM615)

يتناول هذا المقرر الأنشطة البحثية بما في ذلك إدارة المشاريع، وتصميم المشاريع البحثية وتحليلها، والاعتبارات الأخلاقية، والمراجعة السليمة للأدب البحثي، وأفضل الممارسات العلمية، وإعداد الرسالة.

مواضيع متقدمة ومتخصصة في الأمن السيبراني (NGCM697)

يغطي هذا المقرر مواضيع ذات أهمية معاصرة أو خاصة لن يتم إدراجها كجزء منتظم ومستمر من المنهج الدراسي.

مشروع تطبيقي (NGCM698)

يمنح هذا المشروع الذي يتم تنفيذه في مجموعات صغيرة خبرة عملية وتطبيقية لبناء مهارات الطلاب وثقتهم بأنفسهم من خلال العمل على مهام واقعية في بيئة تعاونية.

رسالة الماجستير (NGCM699)

تُظهر رسالة الماجستير قدرة الطالب على تطبيق المعرفة والمهارات المتقدمة المكتسبة في مجال الذكاء الاصطناعي والأساليب الشكّلية للأمن السيبراني لمعالجة مشكلة معقدة في مجال الأمن السيبراني.

4. المقررات الاختيارية:

القرصنة الأخلاقية والدفاع عن الأنظمة (NGCM641)

صُمم هذا المقرر لتعريف الطلاب بأساسيات القرصنة وكيفية أن يصبحوا قراصنة أخلاقيين. يركز المقرر على قواعد حسن السلوك والأخلاقيات المتعلقة بمهاجمة الأنظمة. كما يبين عقلية القراصنة المجرمين وتطورهم. يكتسب الطلاب أيضًا فهمًا أساسيًا وتعليمًا حول عناصر اختراق أنظمة الحاسوب لأغراض واضحة تتمثل في تأمينها من المجرمين. يميز المقرر بوضوح شديد بين القرصنة الإجرامية والقرصنة الأخلاقية، ولا تعلم سوى الأخيرة. ثم تركز الدورة على بعض أساسيات الدفاع عن الأنظمة، بما في ذلك التكوينات والبرامج لمنع الوصول غير المصرح به إلى النظام.

أمن الشبكات والتطبيقات (NGCM642)

يوفر هذا المقرر أساسًا شاملاً لتأمين بيئات الشبكات الحديثة. يتعلم الطلاب الدفاع ضد الهجمات على الشبكات السلكية والشبكات اللاسلكية وتطبيقات الويب. تشمل الموضوعات بروتوكولات الشبكات وعمليات الاستغلال، ونقاط الضعف الشائعة في الويب، وتقنيات



تقييم المخاطر والتخفيف من حدتها. بحلول نهاية المقرر، سيكون الطلاب قادرين على التحليل النقدي وتعزيز أمن البنى التحتية المعقدة للشبكات والتطبيقات.

أمن التقنيات الناشئة (NGCM643)

يتناول هذا المقرر التحديات الأمنية واستراتيجيات الدفاع الخاصة بالتقنيات الناشئة مثل الحوسبة السحابية وإنترنت الأشياء وسلسلة الكتل. ويغطي نماذج أمان الحوسبة السحابية، ونقاط الضعف في إنترنت الأشياء وآليات الحماية، ومبادئ أمان سلسلة الكتل، بما في ذلك التوافق والعقود الذكية والثقة اللامركزية. يتعلم الطلاب تقييم وتنفيذ ضوابط أمنية عملية للأنظمة الموزعة وسريعة التطور.

إدارة المخاطر السيبرانية (NGCM644)

يوفر هذا المقرر أساساً شاملاً لإدارة المخاطر السيبرانية داخل المؤسسات الحديثة. يتعلم الطلاب تطبيق منهجيات تقييم المخاطر النوعية والكمية. يركز المقرر على تحديد مخاطر الأمن السيبراني وتحليلها وترتيبها حسب الأولوية، ووضع خطط لمعالجة المخاطر، ودمج المخاطر السيبرانية في حوكمة المؤسسة واتخاذ القرارات الاستراتيجية. بحلول نهاية المقرر، سيكون المتعلمون قادرين على تقييم المخاطر السيبرانية، وتقييم الضوابط، وتصميم سياسات مستنيرة بالمخاطر تعزز الوضع الأمني للمؤسسات والقطاعات الحيوية.

التحليل الجنائي الرقمي (NGCM645)

يقدم هذا المقرر مقدمة مركزة في علم الجنائية الرقمية، ويغطي تحديد الأدلة والحصول عليها وحفظها وتحليلها عبر الأنظمة والشبكات والذاكرة وبيئات السحاب. يتعلم الطلاب المعايير الجنائية وأساليب التحقيق وتفسير الأدلة وتقنيات إعداد التقارير. يتضمن المقرر مفاهيم أساسية للاستجابة للحوادث لدعم التحليل الجنائي، مما يمكن المتعلمين من إعادة بناء الهجمات وإعداد تقارير جنائية قابلة للدفاع عنها قانونياً من خلال المختبرات العملية وحالات دراسية.

البيانات الضخمة والذكاء الاصطناعي المتقدم (NGCM646)

يستكشف هذا المقرر معالجة البيانات على نطاق واسع ومنهجيات الذكاء الاصطناعي المتقدمة. وهو يغطي تقنيات قواعد البيانات ومبادئ التصميم التي يقوم عليها عالم البيانات الضخمة، بالإضافة إلى التعلم العميق والنماذج التوليدية (VAEs، GANs) والتعلم المعزز. يكتسب الطلاب مهارات لمعالجة مجموعات البيانات المعقدة والاستفادة من الذكاء الاصطناعي لاستخلاص الرؤى وتطوير حلول أمنية ذكية.