



Cyber Security

ماجستير

الأمن السيبراني

في عالم رقمي مليء بالتحديات، أصبح الأمن السيبراني حجر الأساس لحماية الأنظمة والبيانات من التهديدات الإلكترونية المتزايدة.

+1 984 382 6080

VertexUniversity.edu.eu





بوابتك إلى المستقبل الرقمي، حيث يلتقي الابتكار بالتكنولوجيا!

تعد **كلية الحوسبة وتكنولوجيا المعلومات في جامعة فيرتكس** كلية متميزة بالابتكار والتطوير وتسعى إلى إحداث تغيير جوهري في مجالات التكنولوجيا الرقمية، حيث تقدم بيئة أكاديمية متقدمة تهدف إلى إعداد مهندسين ومتخصصين في التكنولوجيا قادرين على قيادة الثورة الرقمية وحل تحديات المستقبل. من خلال برامج أكاديمية مرنة ومتوافقة مع المعايير العالمية، توفر الكلية **درجات البكالوريوس، الماجستير، والدكتوراه** في تخصصات حديثة تلي احتياجات سوق العمل الرقمي المتسارع.

جامعة فيرتكس كلية الحوسبة وتكنولوجيا المعلومات

تعتمد الكلية على منهجية تعليمية متقدمة تجمع بين التعليم الأكاديمي النظري والتطبيق العملي القائم على المشاريع والتجارب الحقيقية، مما يضمن تزويد الطلاب بالمعرفة العميقة والمهارات التقنية المتطورة. تتميز المناهج الدراسية بالاعتماد على التعلم القائم على المشروعات (PBL)، حيث يتفاعل الطلاب مع تقنيات الذكاء الاصطناعي، الأمن السيبراني، وإنترنت الأشياء من خلال تطبيقات عملية تعكس واقع الصناعة.



تضم الكلية نخبة من الأكاديميين والخبراء الدوليين في مجالات الهندسة والتكنولوجيا، ممن يمتلكون خبرة واسعة في التدريس الأكاديمي والعمل البحثي والتطبيقي في كبرى المؤسسات والجامعات العالمية. يساهم أعضاء هيئة التدريس في إعداد مناهج متطورة تعتمد على أحدث الأبحاث والاتجاهات التقنية، مما يمنح الطلاب تجربة تعليمية غنية ومتوافقة مع التطورات العالمية. كما يتم تعزيز عملية التعلم من خلال محاضرات تفاعلية، مشروعات بحثية، وشراكات استراتيجية مع شركات تقنية رائدة، مما يضمن تطوير مهارات الطلاب وتأهيلهم لمتطلبات سوق العمل.

تسعى الكلية للحصول على اعتمادات دولية عالمية، مما يعكس التزامها بتقديم تعليم هندسي تكنولوجي عالي الجودة وفقاً لأعلى المعايير الأكاديمية العالمية. كما توفر الكلية برامج تدريبية لطلبة جامعة فيرتكس مما يؤهلهم للحصول على شهادات مهنية عالمية معترف بها في مجالات مثل أمن المعلومات (CEH, CISSP)، إدارة الشبكات (CCNA, CCNP)، الذكاء الاصطناعي وتحليل البيانات (TensorFlow, AWS AI)، مما يعزز من فرصهم التوظيفية ويمكنهم من المنافسة في سوق العمل. في جامعة فيرتكس، نقدم تجربة تعليمية متكاملة، ونبني المهندسين والخبراء الرقميين القادرين على ابتكار المستقبل. من خلال بيئة أكاديمية متقدمة تعتمد على البحث العلمي، المشاريع التطبيقية، والتكنولوجيا الحديثة، نمنح طلابنا المعرفة، المهارات، والشهادات المهنية التي تمكنهم من تحقيق طموحاتهم المهنية وبناء مستقبل مستدام في عالم الهندسة والتكنولوجيا. انضم إلينا اليوم، وكن جزءاً من الجيل القادم من رواد التكنولوجيا!



في عالم يشهد تطورًا تقنيًا متسارعًا، تسعى كلية الحوسبة وتكنولوجيا المعلومات في جامعة فيرتكس إلى أن تكون مركزًا أكاديميًا عالميًا يدمج بين التعليم الهندسي المبتكر والتكنولوجيا الحديثة. من خلال تقديم برامج تعليمية متقدمة، تعمل الكلية على تأهيل مهندسين وتقنيين قادرين على قيادة التحول الرقمي والمساهمة في تطوير حلول مستدامة تلبي احتياجات المجتمع والصناعة.

نبذة عن ماجستير الأمن السيبراني

تقدم كلية الحوسبة وتكنولوجيا المعلومات بجامعة فيرتكس برنامج ماجستير الأمن السيبراني، الذي يهدف إلى تزويد الطلاب بمعرفة متقدمة في مجال تأمين الأنظمة، تحليل الهجمات الإلكترونية، وتعزيز استراتيجيات الحماية الرقمية. يركز البرنامج على تزويد الدارسين بالمهارات العملية والأدوات التقنية اللازمة لمواجهة التهديدات السيبرانية وحماية البنية التحتية للمؤسسات من المخاطر المتطورة.

يهدف ماجستير الأمن السيبراني إلى بناء قاعدة معرفية متينة في الأمن الرقمي، حيث يتعلم الطلاب كيفية تقييم المخاطر، تصميم الحلول الأمنية المتقدمة، وإدارة أنظمة الحماية بفعالية. كما يتم تزويدهم بمهارات تحليل الهجمات السيبرانية، تطوير استراتيجيات الدفاع السيبراني، وتطبيق معايير الأمن السيبراني الحديثة لضمان حماية البيانات والمعلومات الحساسة. يركز البرنامج على تأهيل متخصصين قادرين على مواجهة التحديات الأمنية الناشئة، مع تعزيز الابتكار والتطوير المستمر في هذا المجال الحيوي.

يولي البرنامج اهتمامًا كبيرًا بالجوانب التطبيقية، حيث يتمكن الطلاب من اختبار مهاراتهم ضمن بيئات محاكاة متقدمة، من خلال مشاريع بحثية ودورات تدريبية متخصصة في تحليل الثغرات الأمنية، واختبار الاختراق، والتصدي للهجمات السيبرانية. كما يتناول البرنامج الجوانب التنظيمية والتشريعية للأمن السيبراني، حيث يتم تدريب الطلاب على الامتثال للمعايير الدولية، السياسات الأمنية، والتشريعات الرقمية، مما يعزز من جاهزيتهم للعمل في بيئات مهنية مختلفة.

يتم تقديم هذا البرنامج من قبل نخبة من الأكاديميين والخبراء المتخصصين في الأمن السيبراني، مما يضمن محتوى تعليمي متجدد يجمع بين الأسس النظرية والتطبيقات العملية. يوفر البرنامج بيئة تعليمية متطورة، تشمل مختبرات متقدمة لمحاكاة الهجمات السيبرانية، ومشاريع بحثية تهدف إلى تطوير تقنيات أمنية جديدة تعزز الحماية المستقبلية للبنية التحتية الرقمية. كما يمنح البرنامج الفرصة للطلاب للحصول على شهادات احترافية معترف بها عالميًا في الأمن السيبراني، مما يعزز فرصهم في سوق العمل ويوفر لهم ميزة تنافسية قوية.

يفتح برنامج ماجستير الأمن السيبراني أمام خريجيه العديد من الفرص المهنية، حيث يمكنهم العمل في وظائف متقدمة مثل محلل أمن المعلومات، مهندس الأمن السيبراني، مختبر اختراق (Ethical Hacker)، خبير التحقيق الرقمي الجنائي، مستشار أمن سيبراني، ومدير أمن المعلومات (CISO). كما يمكنهم الالتحاق بالمؤسسات الحكومية، الشركات التقنية، البنوك، مراكز الأبحاث الأمنية، أو حتى إنشاء مشاريعهم الخاصة في مجال الحلول الأمنية، مما يتيح لهم مستقبلًا مهنيًا واعدًا في عالم الأمن السيبراني.



أبرز محاور التخصص:

– المنظور الوظيفي:

مع تزايد المخاطر الإلكترونية وتعقيد الهجمات السيبرانية، أصبح الأمن السيبراني أحد أكثر التخصصات المطلوبة في سوق العمل. يوفر ماجستير الأمن السيبراني فرصًا مهنية متقدمة في مجالات مثل حماية البنية التحتية الرقمية، إدارة المخاطر السيبرانية، تحليل التهديدات الإلكترونية، والاستجابة للحوادث الأمنية. تعتمد المؤسسات الحكومية، الشركات المالية، ومراكز البحث والتطوير على الخبراء في هذا المجال لضمان أمن أنظمتها الرقمية وحماية بياناتها الحساسة. يمكن



للخريجين العمل في أدوار متقدمة تشمل التحقيقات الرقمية، اختبار الاختراق، وضع استراتيجيات الدفاع السيبراني، وإدارة أمن المعلومات على المستوى المؤسسي.

– المنظر الاستراتيجي:

يعد الأمن السيبراني عنصرًا أساسيًا في استمرارية الأعمال وضمان استقرار المؤسسات في العصر الرقمي. يسعى برنامج ماجستير الأمن السيبراني في جامعة فيرتكس إلى تأهيل الطلاب لفهم طبيعة المخاطر السيبرانية، تطوير استراتيجيات أمنية متقدمة، وتنفيذ سياسات حماية قوية لمكافحة التهديدات المتطورة. من خلال بناء أنظمة دفاعية فعالة، تطبيق معايير الأمن الحديثة، وتحليل الأنماط الهجومية، يساهم الأمن السيبراني في تحسين جاهزية المؤسسات الرقمية، تعزيز ثقة المستخدمين، وحماية المعلومات الحيوية من التسريبات أو الهجمات الإلكترونية المتقدمة.

– التكنولوجيا والابتكار:

يعتمد الأمن السيبراني على استخدام أحدث الأدوات والتقنيات لمواجهة التهديدات السيبرانية المتغيرة. يركز ماجستير الأمن السيبراني على توظيف الذكاء الاصطناعي في كشف التهديدات، تحليل البيانات الضخمة في الأمن السيبراني، تطوير تقنيات التشفير المتقدمة، وتحليل البرمجيات الخبيثة لتعزيز الحماية الرقمية. كما يتعلم الطلاب كيفية تصميم حلول ذكية للأمن السيبراني، تحسين أداء أنظمة الدفاع الرقمي، وتطبيق أحدث استراتيجيات الأمن السيبراني، بما في ذلك الاستجابة التلقائية للحوادث الأمنية، مما يضمن مستوى أمان متقدم للمؤسسات في بيئة تقنية دائمة التطور.

– التعليم التطبيقي:

يوفر البرنامج تجربة تعليمية متكاملة تجمع بين الدراسات النظرية والتطبيقات العملية المتقدمة، حيث يتمكن الطلاب من تطوير مهاراتهم عبر مختبرات محاكاة للهجمات السيبرانية، دورات متخصصة في تحليل الاختراقات، وتنفيذ مشاريع بحثية بالتعاون مع مؤسسات تقنية كبرى. يساعد هذا النهج التطبيقي على إعداد الطلاب لمواجهة التحديات الأمنية الواقعية، تحسين قدرتهم على تصميم أنظمة أمنية قوية، وتطوير الحلول الفعالة لحماية البنى التحتية الرقمية، مما يعزز من جاهزيتهم للعمل في بيئات مهنية متطورة.

– تنمية المهارات:

يركز ماجستير الأمن السيبراني على تطوير مجموعة واسعة من المهارات الاحترافية تشمل:

- تحليل المخاطر السيبرانية وتقييم الثغرات الأمنية للكشف عن نقاط الضعف في الأنظمة الرقمية.
- تصميم استراتيجيات متقدمة للحماية الإلكترونية وتطبيق أحدث التقنيات لضمان أمن الشبكات والبيانات.
- إجراء التحقيقات الجنائية الرقمية للكشف عن التهديدات الإلكترونية وجمع الأدلة الرقمية لتحليل الهجمات.
- إدارة الأمن السيبراني من خلال تطوير سياسات أمنية قوية والإشراف على تنفيذها داخل المؤسسات.
- العمل ضمن فرق متعددة التخصصات لضمان تكامل الحلول الأمنية وحماية البنية التحتية الرقمية بفعالية.

تُعدّ قادة أمن رقمي قادرين على التصدي للتهديدات السيبرانية، بمعايير عالمية واستراتيجيات ذكية.

رسالتنا

تقديم تجربة تعليمية متقدمة تدمج بين التحليل النظري والتطبيق العملي في الأمن السيبراني، لإعداد خبراء يمتلكون أدوات الدفاع الرقمي، تحليل التهديدات، والتصدي للهجمات باستخدام أحدث التقنيات والمعايير العالمية.

رؤيتنا

برنامج رائد يُشكّل منصة أكاديمية متكاملة لإعداد قادة في مجال الأمن السيبراني، يجمعون بين المعرفة المتقدمة والمهارات العملية، وقادرون على حماية الفضاء الرقمي وتطوير حلول أمنية مستدامة على مستوى عالمي.



أهداف برنامج ماجستير الأمن السيبراني



- تزويد الطلاب بالمعرفة المتقدمة في الأمن السيبراني، وتمكينهم من حماية الأنظمة الرقمية والبيانات الحساسة من التهديدات الإلكترونية المعقدة.
- إعداد خبراء متخصصين في الأمن السيبراني قادرين على تلبية متطلبات سوق العمل والمساهمة في تطوير حلول أمنية مبتكرة لحماية المؤسسات من المخاطر السيبرانية المتزايدة.
- تعزيز مهارات تحليل المخاطر الأمنية وتمكين الطلاب من تقييم التهديدات السيبرانية وتطوير استراتيجيات فعالة للاستجابة للحوادث الأمنية وحماية البنية التحتية الرقمية.
- تنمية القدرة على البحث العلمي والتطوير التقني في مجال الأمن السيبراني، وتشجيع الطلاب على إيجاد حلول مبتكرة للتحديات السيبرانية المتقدمة.
- تمكين الطلاب من تطبيق أحدث تقنيات التشفير لحماية البيانات وضمان سلامتها وسريتها، مع التركيز على تطوير خوارزميات تشفير متقدمة تلائم التهديدات المتجددة.
- تأهيل الطلاب لاستخدام الأدوات والتقنيات الحديثة في إدارة وتأمين الشبكات والبنية التحتية الرقمية، بما في ذلك الأنظمة السحابية وإنترنت الأشياء.
- تطوير مهارات اختبار الاختراق وتقييم الثغرات الأمنية للكشف عن نقاط الضعف في الأنظمة الرقمية وتعزيز مستويات الحماية ضد الهجمات الإلكترونية المتقدمة.
- تدريب الطلاب على تحليل البرمجيات الضارة والجرائم الإلكترونية، وفهم أساليب الحماية من الفيروسات والهجمات المستهدفة، مثل هجمات التصيد الاحتيالي والتهديدات المستمرة المتقدمة (APT).
- تعزيز الوعي بالجوانب القانونية والأخلاقية للأمن السيبراني، وتمكين الطلاب من الامتثال للوائح والمعايير الدولية لضمان سلامة البيانات والمعلومات الرقمية.
- تزويد الطلاب بمهارات إدارة الحوادث السيبرانية والاستجابة السريعة للطوارئ الأمنية، مع التركيز على تطوير استراتيجيات احتواء التهديدات والتعافي من الهجمات السيبرانية.
- تنمية مهارات العمل الجماعي والتواصل التقني لتعزيز التعاون بين فرق الأمن السيبراني ومختلف الأقسام التقنية داخل المؤسسات، بهدف تطوير حلول أمنية متكاملة.
- تمكين الطلاب من توظيف الذكاء الاصطناعي وتحليل البيانات الضخمة في الأمن السيبراني، مما يتيح لهم تطوير أنظمة ذكية قادرة على كشف التهديدات والتنبؤ بها.
- إعداد الطلاب لفهم وتطبيق استراتيجيات الأمن السيبراني في بيئات الحوسبة السحابية، مع التركيز على تأمين خدمات الحوسبة المتقدمة وحماية البنى التحتية الافتراضية.
- تمكين الطلاب من العمل على مشاريع بحثية وتطبيقية متقدمة لتعزيز مهاراتهم في تصميم وتنفيذ الأنظمة الأمنية المتطورة، مع التركيز على التقنيات الحديثة مثل Blockchain والأمن الحيوي (Biosecurity).
- توفير فرص تدريب متقدمة بالتعاون مع المؤسسات التقنية والمراكز البحثية، مما يمنح الطلاب خبرة عملية في بيئات عمل حقيقية ويؤهلهم لمواجهة تحديات الأمن السيبراني الواقعية.
- تشجيع التعلم المستمر والتطوير المهني لضمان قدرة الخريجين على التكيف مع التغيرات السريعة في التهديدات السيبرانية، ومواكبة أحدث التطورات في تقنيات الحماية الرقمية.

ماذا يمكنك أن تفعل بحصولك على درجة ماجستير الأمن السيبراني؟



يؤهل ماجستير الأمن السيبراني خريجيه لشغل وظائف متقدمة في مجالات الدفاع الرقمي داخل القطاعات البنكية، التقنية، ومراكز الأبحاث الأمنية.

خريجونا يصنعون الفرق في خطوط الدفاع الرقمية عالية الحساسية حول العالم.

- خبير أمن الحوسبة السحابية
- محلل سلوكيات الهجمات الإلكترونية
- مدير استجابة للحوادث السيبرانية

افتح أبوابك لمسارات مهنية متقدمة في الدفاع السيبراني والقيادة الأمنية الرقمية.

- كبير محلي الأمن السيبراني
- مهندس أمن الأنظمة والبنية التحتية
- مختبر اختراق أخلاقي



- محلل تهديدات استخباراتية
- خبير التحليل الجنائي الرقمي
- مدير أمن المعلومات
- خبير إدارة المخاطر السيبرانية
- خبير تشفير وأمن البيانات
- مستشار أمن سيبراني متقدم
- أخصائي الامتثال والحوكمة السيبرانية
- خبير تطوير برمجيات آمنة
- باحث في مجال الأمن السيبراني
- قائد فرق الأمن السيبراني
- خبير الأمن السيبراني في الذكاء الاصطناعي
- رائد أعمال في الأمن السيبراني
- خبير حماية أنظمة إنترنت الأشياء
- أخصائي أمن البنية التحتية الحيوية

الفئة المستهدفة لبرنامج ماجستير الأمن السيبراني



يستهدف برنامج ماجستير الأمن السيبراني مجموعة متنوعة من الأفراد الراغبين في تطوير مهاراتهم ومعرفتهم في مجال حماية الأنظمة الرقمية والتصدي للتهديدات السيبرانية. تشمل الفئات المستهدفة ما يلي:

- الخريجون الجدد من حملة درجة البكالوريوس في علوم الحاسب، علوم الحاسوب، تقنية المعلومات، الهندسة الكهربائية، أو التخصصات ذات الصلة، والذين يسعون إلى بناء مسار مهني قوي في مجال أمن المعلومات، تحليل المخاطر السيبرانية، وتطوير استراتيجيات الحماية الرقمية.
- المهندسون والمتخصصون العاملون في إدارة الشبكات، اختبار الاختراق، الحوسبة السحابية، التحليل الجنائي الرقمي، والاستخبارات السيبرانية، والذين يطمحون إلى تطوير مهاراتهم التقنية والإدارية وتعزيز قدراتهم في مواجهة التهديدات السيبرانية المتقدمة.
- المهنيون الذين يتطلعون إلى الانتقال إلى قطاع الأمن السيبراني واكتساب المهارات اللازمة للعمل في تقييم المخاطر السيبرانية، تصميم أنظمة الحماية، وإدارة استراتيجيات الدفاع الرقمي.
- أصحاب الشركات الناشئة الذين يسعون إلى تعزيز البنية التحتية الأمنية لأعمالهم، تطوير حلول حماية متقدمة، والاستفادة من تقنيات التشفير والذكاء الاصطناعي في تحسين أمن المعلومات.



الأوراق المطلوبة

- القبول النظامي : أن يكون الطالب المتقدم لبرنامج الدراسات العليا حاصلًا على شهادة البكالوريوس من جامعة موثوقة أو من بلد الطالب.
- حصول المتقدم على درجة البكالوريوس في الأمن السيبراني، علوم الحاسب، هندسة الحاسوب، تقنية المعلومات، أو أي تخصص ذي صلة من جامعة معتمدة.
- إجادة اللغة الإنجليزية إذا كانت لغة التدريس في البرنامج باللغة الإنجليزية، مع اجتياز اختبار اللغة المعتمد.
- القبول المشروط: قد تتيح الجامعة القبول المشروط للمتقدمين لحين استكمال جميع متطلبات القبول (تطبق الشروط والأحكام الخاصة بهذه الفئة).
- تقديم المستندات الرسمية التي تشمل أصل شهادة البكالوريوس وكشف الدرجات، مع صور طبق الأصل.
- تعبئة طلب الالتحاق الإلكتروني عبر بوابة القبول والتسجيل في الجامعة.
- دفع رسوم التسجيل والرسوم الدراسية المقررة وفقًا لأنظمة الجامعة.
- الالتزام بأنظمة ولوائح الجامعة من خلال التوقيع على تعهد رسمي.

الأوراق المطلوبة

- صورة ملونة من شهادة البكالوريوس الصادرة من بلد الطالب "وزارة التعليم العالي".
- صورة ملونة من البطاقة الشخصية للطالب أو العائلية للمطابقة.
- صورة ملونة من جواز سفر الطالب.
- صورة شخصية (4*6) خلفية لون أبيض.
- استكمال بيانات التسجيل و توقيعها من قبل الطالب.



توزيع الساعات المعتمدة:

متطلبات الجامعة	9 ساعة معتمدة
متطلبات الكلية (الحوسبة وتكنولوجيا المعلومات)	3 ساعة معتمدة
متطلبات التخصص (الأمن السيبراني)	9 ساعة معتمدة
المقررات الاختيارية الرئيسية	9 ساعة معتمدة
مشروع	6 ساعة معتمدة
الإجمالي	36 ساعة معتمدة

1- متطلبات الجامعة (9 ساعات معتمدة)

رمز المساق	اسم المساق	الساعات المعتمدة	الوصف
MUV1301	منهجيات البحث العلمي	3	يتناول هذا المقرر الأسس الفلسفية والمنهجية للبحث العلمي على مستوى الدراسات العليا (Scientific Research Methodologies). ويغطي أنواع البحوث ومنهجها الكمية والنوعية والمختلطة (Quantitative, Qualitative & Mixed Methods)، وصياغة مشكلة البحث وأسئلته وفرضياته (Research Problem, Questions & Hypotheses)، ومراجعة الأدبيات المنهجية (Systematic Literature Review)، وتصميم البحث وأساليب جمع البيانات وأخذ العينات (Research Design & Sampling)، والتحليل الإحصائي للبيانات، والصدق والثبات (Validity & Reliability)، وأخلاقيات البحث العلمي (Research Ethics)، وكتابة المقترح البحثي والنشر العلمي (Research Proposal & Academic Publishing).
MUV1302	مقاييس البحث باستخدام الذكاء الاصطناعي	3	يتناول هذا المقرر توظيف أدوات الذكاء الاصطناعي في قياس الإنتاج البحثي وتقييمه وتحليله (Research Metrics & Bibliometrics). ويغطي المؤشرات الببليومترية (Bibliometric Indicators) مثل معامل التأثير (Impact Factor) ومؤشر هيرش (h-index)، وقواعد البيانات العلمية (Scopus, Web of Science, Google Scholar)، وتحليل الاستشهادات والشبكات البحثية (Citation & Co-authorship Network Analysis)، واستخدام أدوات الذكاء الاصطناعي في البحث عن الأدبيات وتلخيصها وتحليل الاتجاهات البحثية (AI-assisted Literature Discovery)، مع مناقشة الاستخدام الأخلاقي والمسؤول لهذه الأدوات في البحث العلمي.



رمز المساق	اسم المساق	الساعات المعتمدة	الوصف
MUV1303	إدارة نظم المعلومات	3	يتناول هذا المقرر مفاهيم نظم المعلومات وتقنياتها ودورها في دعم العمليات الإدارية واتخاذ القرار في المؤسسات (Information Systems Management). ويغطي التخطيط الاستراتيجي لنظم المعلومات (IS Strategic Planning)، وحوكمة تقنية المعلومات (IT Governance) وأطرها مثل COBIT و ITIL، ونظم تخطيط موارد المؤسسات (ERP) ونظم دعم القرار وذكاء الأعمال (DSS & Business Intelligence)، وإدارة البيانات والمعرفة، وإدارة مشاريع نظم المعلومات، وأمن المعلومات وإدارة المخاطر، والتحول الرقمي (Digital Transformation).

2- متطلبات الكلية (الحوسبة وتكنولوجيا المعلومات) (3 ساعات معتمدة)

رمز المساق	اسم المساق	الساعات المعتمدة	الوصف
MTEC2301	برمجة بايثون التطبيقية للمهندسين	3	يهدف هذا المقرر إلى تمكين الطالب من استخدام لغة Python بوصفها أداة تطبيقية لحل المشكلات الهندسية وتحليل البيانات (Applied Python Programming). ويتناول أساسيات اللغة وهياكل البيانات، والبرمجة كائنية التوجه، والتعامل مع الملفات وواجهات برمجة التطبيقات (APIs)، والحوسبة العلمية باستخدام مكتبي NumPy و SciPy، ومعالجة البيانات وتحليلها باستخدام Pandas، وتصوير البيانات (Data Visualization) باستخدام Matplotlib، مع مقدمة في مكتبات تعلم الآلة (scikit-learn) وبيئات العمل التفاعلية (Jupyter Notebooks).



3- متطلبات التخصص (الأمن السيبراني) (18 ساعة معتمدة)

رمز المساق	اسم المساق	الساعات المعتمدة	الوصف
MCYB2301	التعلم الآلي التطبيقي لتحليلات الأمن السيبراني	3	يتناول هذا المقرر تطبيق تقنيات تعلم الآلة (Machine Learning) في تحليل البيانات الأمنية والكشف عن التهديدات السيبرانية (Security Analytics). ويغطي تجهيز البيانات الأمنية واستخراج خصائصها (Feature Engineering) من سجلات الأنظمة وحركة الشبكات، ونماذج التصنيف والعنقدة (Classification & Clustering)، واكتشاف السلوك الشاذ (Anomaly Detection)، وأنظمة كشف التسلل الذكية (ML-based Intrusion Detection)، وتصنيف البرمجيات الخبيثة ورسائل التصيد (Malware & Phishing Detection)، وتقييم النماذج في ظل عدم توازن البيانات (Imbalanced Data)، مع مقدمة في الهجمات على نماذج تعلم الآلة (Adversarial Machine Learning).
MCYB2302	التشفير والاتصالات الآمنة	3	يتناول هذا المقرر الأسس الرياضية والتطبيقية لعلم التشفير وبروتوكولات الاتصال الآمن (Cryptography and Secure Communications). ويغطي التشفير المتماثل وأنماط تشغيله (Symmetric Encryption: AES, Modes of Operation)، والتشفير بالمفتاح العام (Public-Key Cryptography: RSA, ECC)، ودوال التجزئة ورموز مصادقة الرسائل (Hash Functions & MAC)، والتواقيع الرقمية والبنية التحتية للمفتاح العام (Digital Signatures & PKI)، وبروتوكولات تبادل المفاتيح والاتصال الآمن (Diffie-Hellman, TLS 1.3)، وإثباتات المعرفة الصفرية (Zero-Knowledge Proofs)، والتشفير ما بعد الكمي (Post-Quantum Cryptography)، مع تحليل الهجمات على الأنظمة التشفيرية (Cryptanalysis).
MCYB3303	الاختراق الأخلاقي واختبار الاختراق (فرق الاختراق الأحمر)	3	يتناول هذا المقرر منهجيات الاختراق الأخلاقي المتقدم واختبار الاختراق وعمليات الفرق الحمراء (Ethical Hacking, Penetration Testing & Red Teaming) في بيئات مخبرية مصرّح بها. ويغطي أطر الاختبار (PTES, OWASP, MITRE ATT&CK)، وجمع المعلومات والاستطلاع (Reconnaissance)، وتقييم الثغرات واستغلالها (Vulnerability Assessment & Exploitation)، وتصعيد الصلاحيات والحركة الجانبية (Privilege Escalation & Lateral Movement)، ومحاكاة الخصوم (Adversary Emulation)، والتنسيق بين الفريقين الأحمر والأزرق (Purple Teaming)، وإعداد تقارير الاختبار، ضمن الإطار القانوني والأخلاقي للمهنة.



رمز المساق	اسم المساق	الساعات المعتمدة	الوصف
MCYB3304	أمن الشبكات والأنظمة	3	يتناول هذا المقرر حماية الشبكات وأنظمة التشغيل على المستوى المؤسسي (Network and Systems Security). ويغطي معماريات أمن الشبكات وتقسيمها (Network Segmentation)، وجدران الحماية من الجيل التالي (Next-Generation Firewalls)، وأنظمة كشف التسلل ومنعه (IDS/IPS)، والشبكات الافتراضية الخاصة (VPN)، وأمن الشبكات اللاسلكية، ومراقبة الأحداث الأمنية وتحليلها (SIEM & Security Monitoring)، وتقوية أنظمة التشغيل (System Hardening)، ونماذج التحكم في الوصول (Access Control Models)، وأمن الخوادم والنقاط الطرفية (Endpoint Security - EDR)، ومبادئ معمارية الثقة الصفيرية (Zero Trust).
MCYB3305	التحقيقات الجنائية الرقمية والاستجابة للحوادث	3	يتناول هذا المقرر منهجيات التحقيق الجنائي الرقمي وإدارة الاستجابة للحوادث السيبرانية (Digital Forensics & Incident Response - DFIR). ويغطي دورة الاستجابة للحوادث (Incident Response Lifecycle - NIST SP 61-800)، وجمع الأدلة الرقمية والحفاظ عليها (Evidence Acquisition & Chain of Custody)، وتحليل الأقراص والذاكرة والشبكات (Disk, Memory & Network Forensics)، وتحليل السجلات (Log Analysis)، والتحليل الأولي للبرمجيات الخبيثة (Malware Triage)، وصيد التهديدات (Threat Hunting)، واستخدام أدوات مثل Autopsy و Volatility، وإعداد التقارير الجنائية مع مراعاة المتطلبات القانونية.
MCYB4301	هندسة أمن المعلومات وإدارة المخاطر	3	يتناول هذا المقرر هندسة أمن المعلومات وإدارة المخاطر على المستوى المؤسسي (Information Security Engineering & Risk Management). ويغطي مبادئ التصميم الآمن للأنظمة (Security by Design)، والمعماريات الأمنية المؤسسية (Enterprise Security Architecture)، ونمذجة التهديدات (Threat Modeling: STRIDE)، ومنهجيات تحديد المخاطر وتقييمها ومعالجتها (Risk Assessment & Treatment)، وأطر ومعايير الحوكمة والامتثال (ISO/IEC 27001, ISO/IEC 27005, NIST RMF, NIST CSF)، وإعداد السياسات الأمنية، وخطط استمرارية الأعمال والتعافي من الكوارث (BCP & DRP).



4- رسالة الماجستير (6 ساعات معتمدة)

رمز المساق	اسم المساق	الساعات المعتمدة	الوصف
MCYB46P	رسالة ماجستير	6	رسالة بحثية يُعدّها الطالب في المستوى الخامس و السادس تحت إشراف أكاديمي، ويعالج فيها مشكلة بحثية أصيلة في مجال الأمن السيبراني (Master's Thesis). وتتضمن مراجعة منهجية للأدبيات (Literature Review)، وصياغة المشكلة والفرضيات، وتصميم المنهجية وتنفيذ التجارب أو النماذج الأولية (Methodology & Experimentation)، وتحليل النتائج وتفسيرها، وكتابة الرسالة وفق معايير الكتابة الأكاديمية، ومناقشتها أمام لجنة علمية (Thesis Defense)، بما يُظهر قدرة الطالب على البحث المستقل والإسهام في المعرفة.



المستوى	رمز المقرر	اسم المقرر (عربي)	اسم المقرر (English)	الساعات	نوع المتطلب	المتطلب السابق
المستوى الأول (Level 1)	MVTU1301	مناهج البحث العلمي	Scientific Research Methods	3	جامعة	-
	VTU1302	مقاييس البحث باستخدام الذكاء الاصطناعي	Research Metrics Using Artificial Intelligence	3	جامعة	-
	MVTU1303	إدارة نظم المعلومات	Information Systems Management	3	جامعة	-
مجموع ساعات المستوى الأول				9		
المستوى الثاني (Level 2)	MTEC2301	برمجة بايثون التطبيقية للمهندسين	Applied Python Programming for Engineers	3	كلية	-
	MTEC2302	التعلم الآلي التطبيقي لتحليلات الأمن	Applied Machine Learning for Security Analytics	3	كلية	-
	MCYS2303	التشفير والاتصالات الآمنة	Cryptography and Secure Communications	3	برنامج	-
مجموع ساعات المستوى الثاني				9		
المستوى الثالث (Level 3)	MCYS3301	الاختراق الأخلاقي واختبار الاختراق (فرق الاختراق الأحمر)	Ethical Hacking and Penetration Testing (Red Teams)	3	برنامج	التشفير والاتصالات الآمنة
	MCYS3302	أمن الشبكات والأنظمة	Network and Systems Security	3	برنامج	التشفير والاتصالات الآمنة
مجموع ساعات المستوى الثالث				6		
المستوى الرابع (Level 4)	MCYS4301	هندسة أمن المعلومات وإدارة المخاطر	Information Security Engineering and Risk Management	3	برنامج	أمن الشبكات والأنظمة
	MCYS4302	التحقيقات الجنائية الرقمية والاستجابة للحوادث	Digital Forensics and Incident Response	3	برنامج	التعلم الآلي التطبيقي لتحليلات الأمن السيبراني
مجموع ساعات المستوى الرابع				6		
المستوى الخامس (Level 5)	MCYS53P	رسالة ماجستير	Master's Thesis	3	برنامج	-
مجموع ساعات المستوى الخامس				3		
المستوى السادس (Level 6)	MCYS53P	رسالة ماجستير	Master's Thesis	3	برنامج	-
مجموع ساعات المستوى السادس				3		
المجموع الكلي للساعات المعتمدة				36		