جامعة الملك سعود
King Saud University

الدليل الإرشادي لطلاب
ماجستير العلوم في الأمن السيبراني

العام الجامعي 1445هـ / 2023

نبذة عن البرنامج:

تُعد كلية علوم الحاسب والمعلومات بجامعة الملك سعود أول كلية حاسب آلي تم إنشاؤها في المملكة العربية السعودية بتاريخ 1404/5/19هـ، ومنذ ذلك الحين وهي تسعى سعيًا حثيثًا لتحقيق الريادة في التعليم والبحث العلمي في مجالات الحوسبة وتقنية المعرفة من خلال المساهمة ببناء قدرات وطنية متميزة قادرة على صناعة التغيير ومجابهة تحديات الألفية الثالثة، وذلك عن طريق تقديم برامج متنوعة ومعتمدة دولياً في مرحلتي البكالوريوس والدراسات العليا من خلال أقسامها علوم الحاسب وهندسة الحاسب وهندسة البرمجيات ونظم المعلومات وتقنية المعلومات، وحاليًا يتجاوز عدد الطلاب في الكلية 1707 طالبًا و طالبة، ويبلغ إجمالي عدد الخريجين من برامج البكالوريوس من مختلف أقسام الكلية منذ انشائها 5000 متخصص ومتخصصة يعملون في مختلف قطاعات التعليم وتقنية المعلومات.

وتفخر كلية علوم الحاسب والمعلومات ببرامجها الحالية ومخرجاتها، ووعيها والتزامها بدورها المحوري في تنفيذ رؤية المملكة العربية السعودية 2030م، والتي ركزت كثيرًاً على تقوية وتعزيز الأمن السيبراني لحماية البنى التحتية الحيوية الوطنية وأنظمة تقنية المعلومات والاتصالات؛ مما دفعها لتسخير كل أقسامها للتشارك في تقديم برنامج مستقل للماجستير في الأمن السيبراني.

ويلبي برنامج ماجستير العلوم في الأمن السيبراني الحاجة المتزايدة للعاملين المؤهلين تأهيلاً صحيحًا في مجال الأمن السيبراني في المملكة ومنطقة الخليج، والذين باستطاعتهم تلبية احتياجات وتوقعات المنظمات والحكومات للفهم، والاستجابة، والتعافي من الهجمات الأمنية على جميع المستويات؛ حيث يزودهم بإطار عمل ومعرفة لحماية الأصول الإلكترونية للمؤسسة، فالبرنامج مصمم للمهنيين الذين يرغبون بتسليح أنفسهم بالمعرفة والمهارات المطلوبة لمواجهة التحديات التي تفرضها التهديدات السيبرانية المتزايدة، وسيكون البرنامج أيضًا اختيارًا جيدًا لحديثي التخرج من

أي برنامج متعلق بتكنولوجيا المعلومات، فباستخدام نهج متعدد التخصصات صمم البرنامج لتزويد الطلاب بإطار تحليلي واسع لتقييم وحل مشاكل الأمن السيبراني مثل الوقاية، والكشف، والتصدي، والتعافي من الحوادث السيبرانية، ويتعلم الطلاب الأدوات الفنية والممارسات التنظيمية مثل التدريب، والتحكم في الوصول، وجمع الأدلة، واستعادة القدرة على العمل بعد الكوارث، وتخطيط استمرارية العمل.

اسم الدرجة العلمية: ماجستير العلوم في الأمن السيبراني

لغة البرنامج: اللغة الانجليزية

متطلبات الحصول على الدرجة:

- أن يجتاز الطالب (36) وحدة دراسية من مقررات الماجستير متضمنة المشروع البحثي.

الهيكل العام للبرنامج:

عدد الوحدات المطلوبة (36) وحدة دراسية متضمنة مشروع البحث على النحو التالي:

نوع المقررات	عدد المقررات	عدد الوحدات المطلوبة
مقررات إجبارية	5	(15) وحدة دراسية
مقررات اختيارية	5	(15) وحدة دراسية
مشروع البحث	2	(6) وحدات دراسية
المجموع	**12**	**(36) وحدة دراسية**

الخطة النموذجية للبرنامج:

الفصل الأول	الفصل الثاني	الفصل الثالث	الفصل الرابع
501 أمن 502 امن 503 أمن	504 أمن 505 أمن مقرر اختياري (1)	مقرر اختياري (2) مقرر اختياري (3) 598 أمن	مقرر اختياري(4) مقرر اختياري(5) 599 أمن
9 ساعات	**9 ساعات**	**9ساعات**	**9ساعات**

المقررات الإجبارية: على الطلبة اجتياز كل المواد في هذه القائمة:

رقم المقرر	مسمى المقرر	عدد الوحدات الدراسية	متطلب سابق
501 أمن	أساسيات الأمن السيبراني	3 ساعات	
502 أمن	توكيد البرمجيات	3 ساعات	
503 أمن	التشفير التطبيقي	3 ساعات	
504 أمن	حوكمة الأمن السيبراني	3 ساعات	501 أمن
505 أمن	أمن الشبكات	3 ساعات	503 أمن
598 أمن	مشروع بحث (1)	3 ساعات	إكمال 18 وحدة دراسية
599 أمن	مشروع بحث (2)	3 ساعات	598 أمن
المجموع		**21 ساعة**	

المقررات الاختيارية: يختار الطالب خمسة مقررات من المجموعة التالية:

رقم المقرر	مسمى المقرر	عدد الوحدات الدراسية	متطلب سابق
522 أمن	معمل الأمن السيبراني	3 ساعات	501 أمن، 502 أمن، 503 أمن
541 أمن	أمن الأنظمة	3 ساعات	501 أمن
542 أمن	التشفير وتحليل الشفرات المتقدم	3 ساعات	503 أمن
543 أمن	أمن الشبكات والمحيط المتقدم	3 ساعات	505 أمن
544 أمن	الاستجابة للحوادث والتعامل معها	3 ساعات	505 أمن
545 أمن	القانون والامتثال والتدقيق للأمن السيبراني	3 ساعات	504 أمن
546 أمن	الجريمة الإلكترونية والعلوم الجنائية الرقمية	3 ساعات	541 أمن
547 أمن	تحليل نظام الملفات والعلوم الجنائية المتقدمة	3 ساعات	541 أمن
548 أمن	اختبار الاختراق وتقييم الضعف	3 ساعات	505 أمن
549 أمن	هندسة الخصوصية	3 ساعات	503 أمن
550 أمن	أمن قواعد البيانات	3 ساعات	501 أمن
551 أمن	أمن تطبيقات الويب	3 ساعات	502 أمن
552 أمن	أمن الحوسبة السحابية	3 ساعات	541 أمن
553 أمن	النظم المادية السيبرانية	3 ساعات	541 أمن
554 أمن	أجهزة / برمجيات الهندسة العكسية	3 ساعات	541 أمن
555 أمن	أمن الجوال	3 ساعات	505 أمن
556 أمن	موضوعات مختارة في الأمن السيبراني	3 ساعات	501 أمن، 502 أمن، 503 أمن
	المجموع	**15 ساعات**	

إرشادات مهمة للطلبة المستجدين:

نبارك لكم قبولكم في ماجستير العلوم في الأمن السيبراني ونتمنى لكم التوفيق في دراستكم.
يرجى أخذ الملاحظات التالية لتسهيل إجراءات تسجيلكم مقررات البرنامج:

1-يجب تفعيل الإيميل الجامعي الرسمي حيث أن جميع مراسلات البرنامج وإعلاناته ستكون من وإلى الإيميل الرسمي للطالب فقط.

2-يتم تسجيل المقررات الاعتيادية عن طريق بوابة النظام الأكاديمي (Edugate)، وإن وجدت مشكلة، يتم التسجيل يدويًا عن طريق تسليم نموذج تسجيل مقرر لوحدة الشئون الطلابية في عمادة الدراسات العليا.

3-للاستفسارات الأكاديمية، نأمل التواصل مع المرشد والمساعد الأكاديمي:

- للطالبات والطلاب: أ. جوهرة المنيع (gelmenaia@ksu.edu.sa)
- للطالبات والطلاب: أ . نجود القحطاني (nalqhtany@ksu.edu.sa)

4-للاستفسارات الأخرى، نأمل التواصل مع رئيس مجلس البرنامج عبر الإيميل الرسمي (sec@ksu.edu.sa).

5-بالنسبة للطالبات، بإمكانهم مراجعة وحدة الدراسات العليا في الكلية لأي استفسارات أخرى (fccis1gsu@ksu.edu.sa).

إرشادات عامة بمقرر المشروع البحثي:

1-تسجيل مقرر المشروع البحثي 1 يتم عن طريق مجلس البرنامج، وذلك بتعبئة النموذج الخاص الذي يُرسل عادة خلال الفصل الدراسي والذي يشمل قائمة الاهتمامات البحثية لكل عضو هيئة تدريس بالكلية:

- يتواصل الطالب مع أعضاء هيئة التدريس ويتفق مع أحدهم للإشراف على مقرر المشروع البحثي (1)، ومن ثم يتم تعبئة النموذج الخاص وإرساله لمجلس البرنامج.
- بعد انتهاء فترة تعبئة النموذج، يقوم مجلس البرنامج بتوزيع الطلبة على المشرفين حسب رغبة الطالب وموافقة المشرف مع الاخذ بالاعتبار العبء التدريسي الحالي للدكتور المشرف.
- يتم طرح عدد كافي من شعب المشروع البحثي (1) في بداية الفصل الدراسي.
- يقوم الطالب بالتسجيل في شعبة الدكتور المشرف أو أي شعبة أخرى متاحة للتسجيل.
- بعد انتهاء فترة التسجيل، يتم تغيير مدرس الشعبة الى الدكتور المشرف المتفق عليه مسبقا.
- يحذف المقرر عن الطالب الذي يسجل في المقرر بدون اتباع الخطوات السابقة.

2-يجب التقيد في كتابة التقرير الخاص بالمشروع بالنموذج المُعطى من مجلس البرنامج والمتوفر بالموقع الرسمي. على أن تكون كتابة التقرير باللغة الإنجليزية، مع تجنب الأخطاء اللغوية والإملائية في الكتابة (بالإمكان التواصل مع وحدة مساندة الباحثين بعمادة البحث العلمي للتدقيق اللغوي وقياس نسبة التشابه والاقتباس). ويجب ألا تزيد نسبة التشابه في التقرير عن 20%.

3-بعد الانتهاء من المشروع البحثي (1)، يقوم الطالب في الفصل الذي يليه بالتسجيل في مقرر المشروع البحثي (2) في أي شعبة متاحة وسيقوم مجلس البرنامج بتعديل مدرس المقرر الى الدكتور المشرف على كل طالب.

4-يجب التواصل بشكل دوري مع المشرف وتسليم تقارير دورية عن سير المشروع.

5-الحرص على النشر في مجلات ومؤتمرات علمية مُحكمة (خصوصًا وأن الجامعة تغطي تكلفة النشر بمؤتمر وتُقدم للطلبة حوافز للنشر في مجلات مُحكمة تصل لـ 9600 ريال).

مواقع مهمة للطالب:

الجهة	الموقع الإلكتروني
موقع الكلية	https://ccis.ksu.edu.sa/
بوابة النظام الأكاديمي	https://edugate.ksu.edu.sa/
نظام إدارة التعلم	https://lms.ksu.edu.sa/
نظام حضور المؤتمرات	https://eservices.ksu.edu.sa/ACGS/
برنامج دعم النشر العلمي	https://dsrs.ksu.edu.sa/ar/node/2228
وحدة مساندة الباحثين	https://dsrs.ksu.edu.sa/ar/node/623
وحدة مساندة الباحثات	https://dsrs.ksu.edu.sa/ar/node/1117
اعتماد طلبات التخرج	https://eservices.ksu.edu.sa/Graduates/
ايميل لجنة مشاريع التخرج	SEC_Project@ksu.edu.sa
صفحة البرنامج	https://ccis.ksu.edu.sa/ar/node/2145

وسائل تواصل مهمة للطالب:

الجهة	الموقع الإلكتروني
منسقة البرنامج	gelmenaia@ksu.edu.sa_
وكالة الكلية للدراسات العليا والبحث العلمي	ccisgr@ksu.edu.sa
وحدة الدراسات العليا بالكلية (طالبات)	fccis1gsu@ksu.edu.sa
وحدة الشئون الطلابية بعمادة الدراسات العليا	dgsf_sau@ksu.edu.sa

المرشدون الأكاديميون:

	طالبات /طلاب	طالبات/ طلاب
المرشد/المساعد	أ. جوهرة المنيع	أ.نجود القحطاني
إيميل	gelmenaia@ksu.edu.sa	nalqhtany@ksu.edu.sa
مكتب	مبنى 6 الدور الثالث مكتب 150	مبنى 6 الدور الاول مكتب 21

مهام وحدة الشئون الطلابية بعمادة الدراسات العليا:

1-طرح التقويم الأكاديمي الخاص بمواعيد الحركات الأكاديمية لطلبة الدراسات العليا (مواعيد تأجيل الدراسة، وحذف المقررات، وحذف الفصل) وتنفيذها بالنظام الأكاديمي.

2-تنفيذ ومتابعة شؤون التسجيل على النظام الأكاديمي، وتنفيذ قرارات لجنة الشؤون الطلابية.

وصف مقررات البرنامج:

ملاحظة: تم تمثيل الساعات المعتمدة على الشكل التالي: عدد الساعات (محاضرة، معمل)

المقررات الإجبارية		
501 أمن	أساسيات الأمن السيبراني	3(3+0)
يتناول هذا المقرر المفاهيم الأساسية للأمن السيبراني. يستكشف المقرر تقنيات الدفاع الأمني في العمق لتأمين المؤسسة. وتشمل الموضوعات قانون أمن المعلومات والأخلاق؛ الجريمة السيبرانية؛ مفاهيم وآليات الأمن؛ دورة حياة الأنظمة الأمنية؛ المخاطر والهجمات؛ تقنيات الأمن؛ التشفير الأساسي وتطبيقاته؛ العلوم الجنائية الرقمية؛ القياسات البيومترية؛ كشف ومنع الاختراق؛ الأمن المادي والشخصي؛ تطبيق وإدارة الأمن؛ قضايا إخفاء الهوية والخصوصية لأنظمة المعلومات.		
502 أمن	توكيد البرمجيات	3(3+0)
يتطلب تطوير برامج آمنة وقوية تنفيذ منهجيات راسخة في هندسة البرمجيات مع توجيه معين نحو الأمن. يقدم هذا المقرر موضوعات متقدمة في منهجية تصميم وتطوير واختبار البرمجيات الآمنة. وتشمل المواضيع أفضل ممارسات أمن البرمجيات والمنهجيات والتقنيات؛ متطلبات الأمن؛ تحليل المخاطر المعمارية؛ تحليل البرمجيات القائم على الهجمات والدفاعات؛ البرمجة الآمنة؛ نوع السلامة؛ أطر الأمان.		
503 أمن	التشفير التطبيقي	3(3+0)
يغطي هذا المقرر أساسيات تقنيات التشفير وتطبيقاته في أنظمة الحاسب وبروتوكولات الشبكات. تشمل الموضوعات: تقنيات التشفير الكلاسيكية؛ تشفير متماثل؛ كتلة التشفير؛ تيار التشفير؛ مفتاح التشفير العام؛ إدارة المفتاح؛ وظائف التجزئة التشفيرية؛ تطبيقات التشفير في أنظمة الحاسب؛ تطبيقات التشفير في بروتوكولات الشبكات.		
504أمن	حوكمة الأمن السيبراني	3(3+0)
يغطي هذا المقرر القضايا المتعلقة بالإدارة الفعالة لأمن المعلومات في أي مؤسسة. يوفر المقرر المعلومات والإرشادات التي يمكن أن تساعد في إنشاء إطار لضمان أن تتماشى استراتيجيات أمن المعلومات مع أهداف العمل وتكون متماشية مع القوانين واللوائح المعمول بها. يغطي هذا المقرر أيضًا الأطر والنماذج والعمليات والأدوات الحالية لإدارة المخاطر بغرض تزويد الطلاب بالنظرية والعلوم والمعرفة العملية لتنفيذ إدارة المخاطر في المؤسسة.		
505أمن	أمن الشبكات	3(3+0)
يغطي هذه المقرر قضايا أمن البنية التحتية. سوف يتعلم الطلاب التهديدات التي تواجه شبكات الحاسب من خلال استغلال نقاط الضعف في تصميم البنية التحتية للشبكات والعيوب الأمنية في بروتوكولات البنية الأساسية للشبكات. وتشمل المواضيع أمن البريد الإلكتروني؛ DNS؛ خوادم الويب؛ كشف الاختراق؛ هياكل الجدران النارية والشبكات الافتراضية الخاصة؛ التشفير؛ تحديد الهوية والتحكم بإمكانية الوصول؛ بروتوكولات أمن الشبكات.		

المقررات الاختيارية		
522 أمن	معمل الأمن السيبراني	3(0+6)
سوف ينفذ الطلاب ما تعلموه في المقررات السابقة من أجل حماية بيئة ما وتقييم مدى صلابتها ومن ثم محاولة خرقها. إنها فرصة لممارسة تمرينات يدوية في بيئة مخصصة لمعمل الأمن.		
541 أمن	أمن الأنظمة	3(3+0)
يغطي هذا المقرر المواضيع التي تتعلق بتأمين وتقوية أنظمة التشغيل؛ وتأمين البنى التحتية للآلة الافتراضية؛ وحماية البنية التحتية للهوية والدليل؛ وحلول كشف التهديدات؛ والبنية التحتية للشبكة الآمنة.		

المقررات الاختيارية		
542 أمن	التشفير وتحليل الشفرات المتقدم	3(3+0)
يغطي هذا المقرر خوارزميات وبروتوكولات التشفير المتقدمة: برهان عدم المعرفة؛ تحويل غير مدرك؛ حساب آمن متعدد الأطراف؛ النقد الرقمي؛ تقاسم سري؛ تشفير العتبة؛ التشفير المستند إلى الهوية؛ التشفير المستند إلى السمة؛ تقنيات تعزيز الخصوصية؛ جمع ونشر البيانات مع الحفاظ على الخصوصية؛ عدم الكشف عن الهوية؛ الاتصالات المجهولة الهوية؛ بيانات اعتماد مجهولة الهوية؛ توقيعات المجموعة؛ الخصوصية وعدم الكشف عن الهوية في أبنية P2P؛ التحكم في الوصول أو المصادقة / التصديق مع تعزيز الخصوصية، وتقنيات تحليل الشفرات.		
543أمن	أمن الشبكات والمحيط المتقدم	3(3+0)
يغطي هذا المقرر بروتوكولات وتقنيات أمن الشبكة المتقدمة. وتشمل المواضيع أمن الشبكات اللاسلكية. تدابير مضادة لهجمات الحرمان من الخدمة الموزعة؛ اعتبارات جدران الحماية المتقدمة؛ **Honeynets**؛ تطوير سياسة أمن المؤسسات؛ تصميم وتكامل البنية التحتية الأمنية المركبة المعقدة؛ أمن الويب والبريد الإلكتروني؛ أمن شبكة **P2P**؛ وإدارة الثقة. بالإضافة يغطي هذا المقرر القضايا المتعلقة بتحديد متطلبات المنظمة وتنفيذها الحالي لأمن المحيط. سوف يتعلم الطلاب كيفية اقتراح تحسينات وتصميم حل جديد من خلال الاختيار المناسب لتكنولوجيا **NAT**؛ التكنولوجيا والهندسة المعمارية المناسبة لجدار الحماية؛ دمج البروتوكولات والتطبيقات لجدار الحماية؛ تصميم نظام مجرد لجدار الحماية؛ وتصميم جدران حماية ذات توافر وكفاءة عاليين. سوف يتعلم الطلاب أيضا كيفية تحديد أنماط الهجوم وإيقاف المتسلل. سيدرس هذا المقرر على نطاق واسع البروتوكولات المتصلة بالإنترنت؛ وطرق تحليل حركة المرور؛ والأدوات والتقنيات اللازمة لتنفيذ ترشيح المرور والمراقبة؛ وتقنيات منع الاختراق.		
544 أمن	الاستجابة للحوادث والتعامل معها	3(3+0)
يقدم هذا المقرر للطلاب خبرة عملية في التحضير لحوادث أمن الكمبيوتر والاستجابة لها. وتشمل الموضوعات إعداد الاستجابة للحوادث؛ والكشف؛ ورد الفعل؛ والتعافي؛ والصيانة. كما سيتم التطرق إلى عملية استعادة القدرة على العمل بعد الكوارث والتخطيط لاستمرارية الأعمال.		
545 أمن	القانون والامتثال والتدقيق للأمن السيبراني	3(3+0)
يثير الإنترنت العديد من المسائل القانونية في العديد من المجالات. من بين القضايا التي سيغطيها المقرر الخصوصية؛ العقود الكترونية؛ العلامات التجارية وأسماء النطاقات؛ قرصنة البرامج وانتهاكات حقوق النشر؛ حماية المحتوى؛ الاختصاص القضائي؛ القوانين؛ المسؤولية المدنية والجنائية؛ والجريمة السيبرانية، بالإضافة يقدم هذا المقرر المفاهيم الأساسية لعملية تدقيق ومراقبة أمن تكنولوجيا المعلومات التي يتم إجراؤها في مجموعة كبيرة من البيئات. يهدف هذا المقرر إلى تمكين الطلاب من إنشاء وتنفيذ عمليات التدقيق بناءً على مواصفات وبرامج التدقيق المعتمدة.		
546 أمن	الجريمة الإلكترونية والعلوم الجنائية الرقمية	3(3+0)
تهتم العلوم الجنائية الرقمية بالتحليل اللاحق لأنظمة الكمبيوتر التي تم اختراقها بالفعل. تستخدم العلوم الجنائية الرقمية الأدوات والتقنيات لجمع وحفظ الأدلة على جرائم الكمبيوتر. تركز العلوم الجنائية الرقمية على إعادة بناء الأحداث التي أدت إلى إفساد النظام، بغاية استعادة البيانات الهامة، ومساعدة السلطات في تتبع أولئك الذين ربما تسببوا في اختراق الأمن، ومعرفة التقنيات التي يستخدمها المتسللون من أجل تحسين حماية الأنظمة ومنع حدوث انتهاكات مماثلة في المستقبل.		
547 أمن	تحليل نظام الملفات والعلوم الجنائية المتقدمة	3(3+0)
يعلم هذا المقرر التحليل المتقدم لمختلف أنظمة الملفات. يستخدم هذا المقرر أدوات العلوم الجنائية المتقدمة والتدريبات العملية لمساعدة الطلاب على فهم كيفية تخزين البيانات على مستوى نظام الملفات. يتم وضع التركيز على جوانب محددة والتي ستكون ذات قيمة لفاحص العلوم الجنائية.		

المقررات الاختيارية		
548 أمن	اختبار الاختراق وتقييم الضعف	3(3+0)
يقدم هذا المقرر للطلاب المنهجيات والتقنيات والأدوات لتقييم ضعف الأنظمة واختبار اختراقها وإصلاح هذا الضعف وحماية البيئة.		
549 أمن	هندسة الخصوصية	3(3+0)
يقدم هذا المقرر نظرة متعمقة على الخصوصية وقوانين الخصوصية والتقنيات المتعلقة بالخصوصية. سيتعلم الطلاب كيفية هندسة الخصوصية باستخدام الأساليب والأدوات الحديثة لمتطلبات وتصميم واختبار البرمجيات. ويشمل هذا التكامل كيفية جمع وتحليل متطلبات البرمجيات والخصوصية، وكيفية التوفيق بين المتطلبات الغامضة وغير المتسقة والمتضاربة، وكيفية تطوير وتقييم تصميمات البرمجيات المستندة إلى مبادئ الخصوصية المعمول بها، بما في ذلك كيفية تحليل بدائل التصميم لتقليل المخاطر التي تهدد الخصوصية الشخصية. بعد الانتهاء من هذا المقرر، سيعرف الطلاب كيفية دمج الخصوصية في دورة حياة تطوير البرمجيات وكيف، ومتى، تتفاعل مع أصحاب المصلحة المعنيين، بما في ذلك القانونيين والمسوّقين وغيرهم من المطورين من أجل تنسيق تصميمات البرمجيات مع قوانين الخصوصية والممارسات التجارية ذات الصلة.		
550 أمن	أمن قواعد البيانات	3(3+0)
يغطي هذا المقرر مفاهيم وتقنيات أمن قواعد البيانات ويناقش الاتجاهات الجديدة لأمن قواعد البيانات في سياق إدارة معلومات الإنترنت. وستغطي الموضوعات نماذج أمن تطبيقات قواعد البيانات، وتدقيق قواعد البيانات والبيانات، والتحكم في الوصول ل **XML**، وإدارة الثقة وحماية الخصوصية. سيقوم الطلاب بدراسة مبادئ وممارسات تنفيذ أمن قواعد بيانات الكمبيوتر في الشركات والصناعات الحديثة، بما في ذلك مبادئ أمن قواعد البيانات، وتدقيق قواعد البيانات، وتنفيذ الأمن وموثوقية قواعد البيانات.		
551 أمن	أمن تطبيقات الويب	3(3+0)
سوف يتمكن الطلاب من فهم بيئة عميل وخادم الويب، مشكلات الأمن السيبراني في تطبيقات الويب؛ حقن **SQL**؛ حقن **HTTPS**؛ أمان التطبيق إلى التطبيق؛ دورة حياة تطبيقات الويب؛ آلية الأمان والتنفيذ؛ الترميز الآمن؛ أمن تطبيق الوصول المفتوح.		
552 أمن	أمن الحوسبة السحابية	3(3+0)
يقدم هذا المقرر مقدمة إلى الحوسبة الافتراضية؛ عمارة الخدمات الموجهة؛ حافلات خدمة المؤسسات؛ السحابة العامة؛ الخاصة والمختلطة؛ **IaaS**؛ **PaaS**؛ **SaaS**؛ التشفير السحابي؛ بيئات الأمان السحابية؛ دراسات الحالة الأمنية؛ توصيات الأمان؛ التدابير المضادة لأمن السحابة.		
553 أمن	النظم المادية السيبرانية	3(3+0)
محتويات هذا المقرر من منظور النظم المادية السيبرانية (**CPS**) هي النمذجة والتصميم والتحليل. يصف الجزء الأول النمذجة الديناميكية والنمذجة المنفصلة والنمذجة الهجينة والجمع المتزامن مع نموذج الحوسبة المتزامنة من آلة الحالة. الجزء الثاني يشمل وحدة المعالجة المركزية وبناء الذاكرة، الإدخال / الإخراج، وتصميم خوارزمية متعددة المهام والجدولة في الوقت الحقيقي. يصف الجزء الثالث متتابعة المنطق التكافؤي والتحسين، طرق تحليل وسائل الاتصال، إلخ. يناقش الجزء الرابع الموضوعات ذات الصلة بالبحث في **CPS**، لتمكين الطلاب من فهم وإتقان نظرية وطريقة نمذجة وتصميم وتحليل **CPS**.		
554 أمن	أجهزة / برمجيات الهندسة العكسية	3(3+0)
يغطي هذا المقرر أسس برنامج الهندسة العكسية؛ برامج المستوى المنخفض؛ أساسيات ويندوز؛ أدوات الهندسة العكسية؛ ثنائيات برنامج التدقيق؛ عكس البرامج الخبيثة؛ كسر الحماية؛ التفريغ، مقدمة في اختراق الأجهزة؛ الهندسة العكسية في الأجهزة.		

المقررات الاختيارية		
555 أمن	أمن الجوال	3(3+0)
يغطي هذا المقرر الأنظمة الأساسية للجوّال والتنفيذ؛ فهم التطوير في نظامي Android وiOS؛ نموذج الأمن OWASP؛ تهديدات أمن الجوّال؛ حماية المعلومات؛ تكوين نظام الأمن الأساسي؛ تحديد أولويات التهديدات، عيوب الخداع في البرامج الضارة؛ التحقق الآمن من الإدخال؛ تعقب تدفق بيانات الجوّال.		
556 أمن	موضوعات مختارة في الأمن السيبراني	3(3+0)
يغطي هذا المقرر المنهجيات والتقنيات والأطر الناشئة حديثا وغيرها للأمن السيبراني، والتي قد لا يتم تضمينها في مكان آخر في المنهج الدراسي.		

مشروع البحث		
598 أمن	مشروع البحث (1)	3(3+0)
سيقوم الطلاب بإجراء مشروع بحث مستقل في مجال الأمن السيبراني. يمكن أن يكون المشروع البحثي إما دراسة لموضوع نظري أو موضوعي (تطوير). ومن المتوقع ان يقدم الطالب عرضا (عمومي) وتقريرا عن نتائج الأبحاث في نهاية المقرر.		
599 أمن	مشروع البحث (2)	3(3+0)
سيقوم الطلاب بإجراء مشروع بحث مستقل في مجال الأمن السيبراني. يمكن أن يكون المشروع البحثي إما دراسة لموضوع نظري أو موضوعي (تطوير). قد يكون هذا المشروع استمرارًا للعمل البحثي الذي تم تنفيذه في المشروع I. من المتوقع أن يقوم الطالب بتقديم عرض (عمومي) وتقرير عن نتائج البحث في نهاية المقرر.		