وصف المواد الدراسية لبرنامج بكالوريوس الأمن السيبراني

رقم المادة	وصف المواد
11000	**فحص مستوى مهارات الحاسوب** **متطلب سابق: –** **عدد الساعات المعتمدة: 0** يجب أن يشمل الامتحان جميع المواضيع التي تدرس في مادة (**11100**) مهارات الحاسوب. على الطلبة اجتياز هذا الامتحان ليتمكنوا من تسجيل مادة (11102) مقدمة في علم الحاسوب. إذا لم يتمكن الطالب من اجتياز هذا الامتحان فعليه إلزامياً تسجيل مادة (11100) مهارات حاسوب – استدراكي (11100) قبل أن يتمكن من تسجيل مادة (**11103**).
11100	**مهارات حاسوب (استدراكي)** **متطلب سابق: –** **عدد الساعات المعتمدة: 0** يهدف هذا المقرر إلى تطوير قدرات الطلبة لاستخدام الحاسوب في مجالات الحياة المتعددة .يقدم هذا المساق المفاهيم الأساسية في الحاسوب، وأساسيات استخدام أنظمة تشغيل الحواسيب الشخصية المعتمدة على الواجهة الرسومية وأساسيات تطبيقات البرامج المكتبية مثل معالجة النصوص والجداول الإلكترونية والعروض التقديمية .بالإضافة لأساسيات استخدام البريد الإلكتروني وتصفح الشبكة العنكبوتية .في نهاية هذا المقرر، من المتوقع أن يكون الطلبة قادرون على استخدام الحواسيب الشخصية لإنجاز المهام اليومية.
11102	**مقدمة في علم الحاسوب** **متطلب سابق: –** **عدد الساعات المعتمدة: 3** يهدف هذه المقرر إلى تقديم المفاهيم الأساسية للبرمجة وعلم الحاسوب .يشمل المقرر تقديما للموضوعات التالية :أنظمة العد تخزين البيانات العمليات على البيانات حل المسائل باستخدام المنطق التسلسلي وحل المسائل باستخدام القرارت والتكرارات، حل المسائل بطريق تراكبية، اساسيات تراكيب البيانات مثل المصفوفات .بالإضافة لمقدمة في البرمجة بإحدى لغات البرمجة عالية المستوى.
11103	**البرمجة البنائية** **متطلب سابق: 11102** **عدد الساعات المعتمدة: 3** يهدف هذه المقرر إلى تقديم المفاهيم الأساسية للبرمجة البنائية باستخدام احدى لغات برمجة الحاسوب عالية المستوى .تشمل الموضوعات :المفاهيم الأساسية للبرمجة البنائية، تصميم البرامج، تطوير وتنقيذ وفحص وتصويب أخطاء البرامج .قواعد اللغة والمعنى للغة البرمجة المستخدمة ليتمكن الطلبة من تطوير البرامج باستخدامها .اساسيات اللغة :المتغيرات، الثوابت أنواع، البيانات .أساسيات الادخال والإخراج .عبارات التكرار والعبارات الشرطية .الدوال أو (المناهجات)، تمرير المعاملات .الخوارزميات الذاتية .المراجع والمتغيرات الديناميكية .أساسيات تراكيب البيانات :المصفوفات، السلاسل الحرفية، السجلات .قراءة الملفات وكتابتها، التصانيف

	ومبادئ البرمجة الكينونية. في نهاية المقرر، من المتوقع أن يكون الطلبة قادرين على تحليل المشاكل الحاسوبية وتصميم وتنفيذ حلول باستخدام إحدى لغات البرمجة عالية المستوى.
11151	**مختبر البرمجة البنائية** **متطلب متزامن بالرقم الجديد: 11103** **عدد الساعات المعتمدة: 1** يهدف هذه المقرر إلى بناء مهارات عملية في البرمجة البنائية باستخدام احدى لغات برمجة الحاسوب عالية المستوى. في نهاية المقرر، من المتوقع أن يكون الطلبة قادرين على تحليل المشاكل الحاسوبية وتصميم وتنفيذ حلول باستخدام إحدى لغات البرمجة عالية المستوى.
15110	**اساسيات الأمن السيبراني** **متطلب سابق: 11102** **عدد الساعات المعتمدة: 3** يهدف هذا المقرر إلى تزويد الطلاب بمعرفة شاملة لمبادئ وممارسات أمن أنظمة المعلومات. وتشمل الموضوعات نظرة عامة على مصطلحات الأمن (التهديدات، الهجمات، الآليات والخدمات الأمنية بما في ذلك السرية والنزاهة والتوفر وغيرها)، وأساسيات نظرية الأعداد (الأعداد الأولية، العمليات الأساسية، حساب الباقي)، والتشفير (التشفير التقليدي، التشفير المتماثل، التشفير غير المتماثل)، ومصادقة المستخدم، والتحكم في الوصول، وأنظمة دفاع سيبرانية (أنظمة الكشف عن التسلل وأنظمة الوقاية وجدران الحماية)، والبرامج الخبيثة، والتخزين الافتراضي) مفهوم التخزين الافتراضي وآليات تثبيت وتكوين نظام التشغيل (**Windows/Linux**) في التخزين الافتراضي مع نهاية هذا المقرر الدراسي، من المتوقع أن يكون الطلاب على دراية بمفاهيم حماية البنية التحتية للحوسبة من التهديدات والهجمات السيبرانية.
15200	**البرمجة للأمن السيبراني** **متطلب سابق: 11103** **عدد الساعات المعتمدة: 3** يهدف هذا المقرر إلى تقديم لغة برمجة حديثة مناسبة لمحترفي الأمن. تتضمن الموضوعات التالية: التحكم في التدفق والسلاسل والقوائم والمجموعات والملفات والوظائف والوحدات النمطية والحزم. الإخراج والإدخال: معالجة الملفات، ميزات البرمجة الموجهة للكائنات: الفئات والكائنات والميراث والتحميل الزائد للمشغل والأخطاء والاستثناءات والتعبيرات العادية والخيوط المتعددة والوحدات النمطية للتعامل مع البيانات متعددة الأبعاد. الشبكات: وحدة مأخذ التوصيل، مسح المنفذ، استكشاف الحزم، تحليل حركة المرور، حقن حزمة **TCP**، تحليل السجل. عمليات الاتصال (**HTTP**) مع المكتبات الأساسية، الاتصالات على شبكة الإنترنت مع وحدة الطلبات، والتحقيقات الجنائية: تحديد المواقع الجغرافية، واستعادة العناصر المحذوفة، وفحص البيانات الوصفية وتسجيل النوافذ. في نهاية هذا المساق، من المتوقع يكون الطلاب قادرين على التعامل مع المشاكل الأمنية باستخدام لغة الاشياء.

15201	**مختبر البرمجة للأمن السيبراني** **متطلب متزامن: 15200** **عدد الساعات المعتمدة: 1** يهدف هذا المقرر إلى ممارسة المفاهيم والنماذج الرئيسية للبرمجة الكيتونية، مع التركيز على تعريف واستخدام الاصناف جنبًا إلى جنب مع أساسيات التصميم للبرمجة الكيتونية. وتشمل الموضوعات ممارسة الاصناف والكائنات، التغليف، التكوين، تخصيص الذاكرة الديناميكية، الميراث، تعدد الأشكال واضافة تعريفات للعمليات. في نهاية هذا المساق، من المتوقع أن يكون الطلاب على دراية بالمبادئ والمفاهيم الرئيسية المتعلقة بالبرمجة الكيتونية. حيث يمكنهم الكتابة والبناء تتبع وتصحيح واختبار برامجهم. بالإضافة إلى استخدام الاصناف المبنية في مشاريع مختلفة.
11213	**تركيب البيانات والخوارزميات للأمن السيبراني** **متطلب سابق: 15200** **عدد الساعات المعتمدة: 3** يهدف هذه المقرر إلى وصف وشرح وتنفيذ أنواع البيانات المجردة، بما في ذلك القوائم والمكدسات وقوائم الانتظار والأشجار والأكوام والمجموعات والخرائط وجداول التجزئة والرسوم البيانية. تصميم وبرمجة مجموعة متنوعة من خوارزميات البحث والترتيب. تصميم خوارزميات ذاتية الاستدعاء (**Recursion**). تحليل كفاءة الوقت والمكان لهياكل البيانات والخوارزميات وتطبيق هذا التحليل لاختيار أفضل بنية بيانات لحل مشاكل معينة. يغطي هذا المقرر تقنيات حل المشكلات العامة، بما في ذلك تقنية التجربة والخطأ، والتقنيات الجشعة، والبرمجة الديناميكية. في نهاية هذا المقرر، يجب أن يكون الطالب قادرًا على اختيار هياكل البيانات المناسبة واستخدام أساليب التصميم المناسبة لكتابة الخوارزميات لمشكلة معينة.
11223	**مبادئ قواعد البيانات** **متطلب سابق: 15200** **عدد الساعات المعتمدة: 3** يهدف هذ المساق إلى تقديم أساسيات تصميم وتنفيذ أنظمة قواعد البيانات. تشمل المواضيع المفاهيم الأساسية لقواعد البيانات، مكونات نظام إدارة قواعد البيانات، بناء نموذج للعلاقات، قواعد البيانات العلاقية، القيود لتحقيق سلامة قاعدة البيانات، الجبر العلاقي، لغات الاستعلام، الصيف المعيارية، تصميمات المخططات، وازالة تكرار البيانات. في نهاية المساق، من المتوقع أن يكون لدى الطلاب معرفة جيدة بمبادئ ومفاهيم قواعد البيانات وكيفية تطبيقها في أنظمة قواعد البيانات الحقيقية.

11335	**أنظمة التشغيل** **متطلب سابق: 11213** **عدد الساعات المعتمدة: 3** يهدف هذه المقرر إلى تقديم المفاهيم الأساسية لتصميم وتنفيذ نظم التشغيل، كما ويغطي العديد من المفاهيم المتعلقة بمعظم أنظمة التشغيل الفعلية. في هذا المقرر، سوف يستكشف الطلاب أهمية نظام التشغيل ووظيفته. تشمل الموضوعات: نظرة عامة على أنظمة التشغيل الحديثة وأنواع أنظمة التشغيل وهياكل أنظمة التشغيل وإدارة العمليات والخيوط (مفاهيم الاتصال والتزامن والتوقف التام) وجدولة وحدة المعالجة المركزية وإدارة الذاكرة والذاكرة الافتراضية وأنظمة الملفات؛ أنظمة الإدخال / الإخراج؛ الأمن والحماية. يتم تنفيذ بعض المواضيع في هذا المقرر عن طريق كتابة البرامج لمعرفة كيف تعمل بشكل عملي. في نهاية هذا المقرر، من المتوقع أن يكون الطلاب على دراية بالعديد من المبادئ والمفاهيم المتعلقة بمعظم أنظمة التشغيل الفعلية وكيف يتم تطبيقها في أنظمة تشغيل حقيقية.
15220	**اساسيات الشبكات** **متطلب سابق: 15110** **عدد الساعات المعتمدة: 3** يهدف هذا المقرر إلى فهم مختلف جوانب الاتصالات بيانات وأنظمة شبكات الحاسوب. ويعد هذا المقرر الأول في مجال شبكات الاتصالات بيانات، وتشمل موضوعات مثل مبادئ نماذج الشبكات والعمليات الأساسية وتحليل الأداء. تشمل الموضوعات مبادئ النقل والشبكات، والنماذج الشبكية) نموذج **TCP / IP** ونموذج(**OSI** ، وتقنيات إشارة البيانات (تماثلية ورقمية)، ووسائط الإرسال والطبقة الفيزيائية، وطبقة الربط بالبيانات (مبادئ، تشكيل، التحكم في الأخطاء والتدفق، بروتوكولات ربط البيانات، والماك الفرعية وتخصيص القناة)، وأجهزة الشبكة، وطبقة الشبكة (التواصل بين الشبكات): بروتوكولات/عناوين بروتوكول الإنترنت، بروتوكولات التوجيه وإعادة التوجيه، وطبقة التطبيق) المقدمة، معماريات العميل والخادم/نظير إلى نظير، بروتوكولات بما في ذلك **HTTP** و **FTP** و **DNS** وغيرها(، ومبادئ شبكات الاتصال اللاسلكية .بحلول نهاية المقرر، سيكون لدى الطلاب فهمًا قويًا لشبكات الحاسوب ومكوناتها وتقنيتها الأساسية. سيكونون قادرين على تصميم وتنفيذ شبكات حاسوب أساسية، بما في ذلك إعداد أجهزة الشبكة ومراقبة أداء الشبكة. كما سيكونون قادرين على تشخيص مشاكل الشبكة وأداء صيانة الشبكة.

15261	**تصميم وتطوير الويب الآمن** **متطلب سابق: 15200** **عدد الساعات المعتمدة: 3** يقدم هذا المقرر الشامل للطلاب مبادئ أساسية في تصميم الويب وبرمجة الإنترنت وأمان الويب. يغطي المقرر جوانب مختلفة من تصميم الويب والبرمجة والأمان، بما في ذلك التهديدات المحتملة والثغرات الأمنية وأفضل الممارسات للتخفيف من مخاطر الأمان. تتضمن الموضوعات: هيكلية تطبيقات الويب، مبادئ تصميم الويب، التصميم المتجاوب، لغات البرمجة على جانب العميل وجانب الخادم مثل (**HTML, CSS, JavaScript, PHP**)، ممارسات الترميز الآمنة، التحقق من صحة الإدخال وتطهيره، آليات المصادقة والتفويض، وإدارة الجلسات. يستكشف المقرر أيضًا معايير وبروتوكولات أمان الويب مثل (**HTTPS, SSL/TLS, OWASP**)، يتعمق المقرر في دراسة الثغرات الأمنية الشائعة والهجمات على الويب، مثل حقن **SQL** والبرمجة النصية عبر المواقع (**XSS**) وطلبات تزوير عبر المواقع (**CSRF**) والنقر المزيف. مع نهاية المقرر، سيكون لدى الطلاب فهم قوي لمبادئ تصميم الويب وبرمجة الإنترنت والأمان، مما يتيح لهم تصميم وتطوير تطبيقات الويب المرئية والفعالة بفعالية وتأمينها.
15262	**مختبر تصميم وتطوير الويب الآمن** **متطلب متزامن: 15261** **عدد الساعات المعتمدة: 1** يوفر هذا المقرر العملي للطلاب تجربة عملية في تصميم وتطوير وتأمين تطبيقات الويب. يغطي مبادئ تصميم الويب ولغات البرمجة وممارسات الترميز الآمن ومعايير أمان الويب. تركز التمارين العملية على مبادئ تصميم الويب ولغات البرمجة على جانب العميل وجانب الخادم مثل (**HTML, CSS, JavaScript, PHP**)، ممارسات الترميز الآمن والتحقق من الإدخال وتطهيره وآليات المصادقة والتفويض وإدارة الجلسات، وتعلم كيفية تحديد وتقليل المخاطر المشتركة للضعف والهجمات على مستوى الويب، مثل حقن **SQL** والبرمجة النصية عبر المواقع (**XSS**) والطلبات المزيفة عبر المواقع (**CSRF**) والنقر الخداعي.(**clickjacking**)

15310	**التشفير** **متطلب متزامن: 15200 + 20234** **عدد الساعات المعتمدة: 3** يقدم هذا المقرر الدراسي مبادئ وممارسات التشفير. سيتعلم الطلاب المفاهيم الأساسية للتشفير وفك التشفير وبروتوكولات التشفير المستخدمة لتأمين الاتصالات الرقمية. تشمل الموضوعات التي يتم تناولها في هذا المقرر: نظرية الأعداد، مصطلحات التشفير، التاريخ وأنواع التشفير. تشفير المفتاح المتماثل: معيار تشفير البيانات (**DES**)، معيار التشفير المتقدم (**AES**)، أنماط تشغيل تشفير الكتلة. تشفير المفتاح غير المتماثل: أنظمة تشفير (**RSA**)، برتوكول (**Diffie–Hellman**)، نظام تشفير الجمل (**ElGamal**). وظائف تجزئة التشفير: طريقة اختزال الرسالة (**MD5**)، خوارزمية التجزئة الآمنة (**SHA**). التوقيعات الرقمية: خوارزمية التوقيع الرقمي (**RSA**)، خوارزمية التوقيع الرقمي (**DSA**)، مخططات التوقيع الرقمي (الجمل). تحليل الشفرات: الهجمات على أنظمة التشفير وتقنيات تحليل التشفير وإدارة المفاتيح. سيشمل المقرر أيضًا تمارين عملية للسماح للطلاب بتنفيذ وتحليل خوارزميات التشفير. مع نهاية هذا المقرر، سيكون لدى الطلاب فهم قوي لمبادئ وممارسات التشفير وسيكونون قادرين على تصميم وتنفيذ وتحليل خوارزميات التشفير للاتصالات الآمنة.
15312	**أمن قواعد البيانات** **متطلب سابق: 11223** **عدد الساعات المعتمدة: 3** هذا المقرر سيوفر نظرة عامة على مفاهيم وتقنيات أمان قواعد البيانات. ستشمل المواضيع مفاهيم أمان قواعد البيانات، الهيكلة الأمنية لقواعد البيانات، المصادقة: إدارة المستخدمين، الملفات الشخصية، وسياسات كلمات المرور. الصلاحيات: الامتيازات، الأدوار، مقدمة لـ **PL/SQL** ومواضيع متقدمة في **PL/SQL** (المؤشرات والمشغلات المؤقتة)، قاعدة بيانات افتراضية خاصة (**VPN**)، التدقيق، تشفير قاعدة البيانات، تشفير البيانات الشفافة. تغطي المساق أيضًا مواضيع متقدمة مثل قضايا أمان إدارة قواعد البيانات مثل تأمين نظام إدارة قواعد البيانات، فرض ضوابط الوصول، والقضايا ذات الصلة.
15313	**مختبر أمن قواعد البيانات** **متطلب متزامن: 15312** **عدد الساعات المعتمدة: 1** يهدف هذا المساق إلى تقديم تصميم وإنشاء قواعد البيانات باستخدام (**DBMS**) يتم التركيز على نمذجة البيانات وإنشاء الجداول والاستعلامات وعرض البيانات والضوابط. وفي نهاية المادة، يجب أن يكون الطلاب قادرين على تصميم وتنفيذ وتقييم هياكل قواعد البيانات الآمنة من خلال إنشاء جداول بسيطة واستعلامات.

15321	**أمن الشبكات والبرتوكولات** **متطلب سابق: 15220 + 15310** **عدد الساعات المعتمدة: 3** يوفر هذا المساق دراسة شاملة في مجال أمن الشبكات والبروتوكولات، حيث تقدم للطلاب معرفة واسعة بالقصور الأمني للشبكات والتهديدات المحتملة. يشمل المنهج الدراسي للمساق مجموعة متنوعة من بروتوكولات الأمن مثل (**SSL/TLS, IPsec, VPNs, SCTP**)، بالإضافة إلى استكشاف أهمية الوصول للمراقبة والترخيص وأنظمة مكافحة الفيروسات وتصفية المحتوى. سيتم القيام بدراسة مفصلة لتكنولوجيا الجدران النارية وأنظمة الكشف عن التسلل، ودور المتسللين والبرامج الضارة. سيغطي المساق المنطقة المتزايدة الأهمية لأمن الإنترنت للأشياء وأمن الشبكة اللاسلكية لأجهزة الاستشعار واستخدام أدوات فحص الشبكة بكفاءة. سيتم النظر في جوانب أداء الشبكة مثل التحكم في الازدحام وجودة الخدمة، بالإضافة إلى مبادئ إدارة الشبكة من خلال (**SNMP**). من خلال تقديم منظور تاريخي ومعاصر للتهديدات الإلكترونية، يهدف المساق إلى تجهيز الطلاب بفهم شامل لإجراءات أمن الشبكة، مما يعدهم لتصميم وتنفيذ وإدارة الشبكات الآمنة في سياقات تكنولوجيا المعلومات المختلفة.
15322	**مختبر أمن الشبكات وبرتوكولاتها** **متطلب متزامن: 15321** **عدد الساعات المعتمدة: 1** يهدف هذا المختبر الشامل إلى دراسة وممارسة التقنيات والبروتوكولات الشائعة لأمن الحواسيب والشبكات. وتتضمن الموضوعات العملية على الأجهزة الشبكية (المحولات، الموجّهات، نقاط الوصول، جدران الحماية، نظم الكشف عن التسلّل / الوقاية منه، المكررات/ المراكز، بطاقات الشبكة)، بناء شبكة محلية صغيرة باستخدام توصيلات واتصالات سليمة، استخدام برنامج (**Packet Tracer**) لتطوير وتهيئة ومحاكاة طوبولوجيا الشبكة ذات الحجم الصغير / المتوسط واستخدام مكوّنات الشبكة النشطة المختلفة، تكوين الشبكات الافتراضية الخاصة(**VLANs**) ، **NATs**، **DHCP**، و**VPNs** ، تطبيق بروتوكولات الإنترنت والتوجيه المختلفة، استخدام وتكوين جدران الحماية / نظم الكشف عن التسلّل، تثبيت وتكوين نظام التشغيل للخادم لتطبيق عدة سياسات أمنية، تثبيت واستخدام **Microsoft Azure** لإنشاء ومراقبة تطبيقات السحابة. بالإضافة إلى استخدام بعض الأدوات الأخرى لاختبار ومراقبة وتوثيق الشبكات السلكية واللاسلكية. كما سيقوم الطلاب أيضًا بإعداد سيناريوهات في مختبر الاختبار الحقيقي، وجمع وتحليل النتائج، وكتابة تقارير المعمل حول التجارب.

15350	**الذكاء الاصطناعي وتحليلات البيانات** **متطلب سابق: 20134 + 20233** **عدد الساعات المعتمدة: 3** يهدف هذا المقرر إلى تعريف الطلاب بتقنيات الذكاء الاصطناعي واعتمادها في النظام (أي الشبكة) للتقوية / دفاع واكتشاف الشذوذ (تطبيق **(IDS/IPS)**. تشمل الموضوعات: مقدمة إلى الذكاء الاصطناعي، الشبكات العصبية، أنظمة المنطق الضبابي، خوارزميات التعلم الآلي، تحديد التهديدات / المخاطر، السلوك، التقييم والتحليل، تحليلات البيانات / الهجوم، التقاط حركة مرور الشبكة، أداة **Wireshark**، ذكاء الأمان، مقاييس الأداء (مقاييس النظام)، والبحث عن التهديدات. كما يقدم هذا المقرر مفهوم التهرب من أنظمة الكشف الذكية وتسميمها التي توفر مراقبة / تحليلًا محسّنًا لحركة مرور الشبكة ، وتساعد في تقليل التعرض (سطح الهجوم والمتجهات) ، وتحسين توافر النظام.
15361	**تحليل وتصميم النظم الأمنه** **متطلب سابق: 11223** **عدد الساعات المعتمدة: 3** في هذا المقرر، سيتعلم الطلاب أهمية دمج الأمان في جميع مراحل دورة حياة تطوير البرمجيات، بما في ذلك جمع المتطلبات والتصميم والتنفيذ والاختبار والتوزيع. تشمل الموضوعات: نمذجة التهديدات، تقنيات البرمجة الآمنة، مبادئ التصميم الآمن، التحقق من صحة الإدخال، ترميز الإخراج، المصادقة والتفويض، إدارة الجلسة، معالجة الأخطاء، التسجيل والرصد، واختبار الأمان. يتم التركيز على الممارسات والأنماط التي تقلل أو تلغي انتهاكات الأمان في النظم المكثفة للبرمجيات، واختبار النظم للكشف عن الضعف الأمني. بنهاية المقرر، سيكون لدى الطلاب المعرفة والمهارات اللازمة لتصميم وتطوير نظم البرمجيات الآمنة، مما يقلل بفعالية من المخاطر المرتبطة بالثغرات الشائعة وعيوب التصميم. يتضمن المقرر أفضل الممارسات الصناعية، بما في ذلك قائمة أفضل عشرة مشروعات لأمان تطبيقات الويب المفتوحة **(OWASP)** و"تجنب أفضل عشرة عيوب تصميم الأمان للبرمجيات" من الجمعية الكهربائية والإلكترونية **(IEEE)**.
15381	**أمن البنية التحتية باستخدام لينكس** **متطلب سابق: 11335** **عدد الساعات المعتمدة: 3** يقدم هذا المقرر لمحة عامة عن أمن البنية التحتية باستخدام نظام لينكس. سيغطي المقرر الموضوعات التالية: عمليات الأمان الرئيسية لنظام لينكس، وحدات أمان لينكس**(LSM)** ، تقوية نواة لينكس والنظام، وأمان البنية التحتية لتأمين المكونات باستخدام لينكس، مثل **VPN** لينكس (الموقع-الموقع والوصول عن بُعد)، جدران الحماية، الموجهات، والمفاتيح. أمان الخادم، بما في ذلك أفضل الممارسات لتأمين خوادم لينكس (إصلاح الثغرات، والتحكم في الوصول، واكتشاف التسلل). المراقبة والتدقيق **(Linux AAA)**، بما في ذلك الأدوات والتقنيات المستخدمة في مراقبة وتدقيق أنظمة لينكس (إدارة السجلات وفحص الثغرات الأمنية). تشمل خدمات الأمان الويب والملفات والبريد ومركز البيانات وشهادات الهيئة المصدرة

	وخدمات النطاق (DNS) وإدارة الأجهزة والتطبيقات المحمولة .(MDM/MAM) طوال المقرر، سيشارك الطلاب في تمارين عملية في المختبر لتطبيق المفاهيم والتقنيات التي تم تعلمها في هذا المقرر. مع نهاية هذا المقرر، سيكون الطلاب قد اكتسبوا خبرة عملية في تأمين مكونات البنية التحتية لنظام لينكس وسيكونون قادرين على تصميم وتنفيذ وتقييم حلول أمان لينكس لمختلف التطبيقات.
15382	**التدقيق والسياسات والتشريعات والأخلاقيات والالتزام بها** **متطلب سابق: 15312** **عدد الساعات المعتمدة: 3** يقدم هذا المقرر نظرة عامة على قضايا السياسة والقانون والأخلاق والامتثال ذات الصلة بمتخصصي الأمن السيبراني. سيغطي المقرر المواضيع التالية: أفضل ممارسات أخلاقيات العمل في مجال الأمن السيبراني للمنظمات والأفراد، القضايا المتعلقة بأخلاقيات وممارسات استخدام منصات التواصل الاجتماعي، التشريعات الوطنية والدولية لمكافحة الجرائم الإلكترونية، السلطات القضائية، الاتفاقيات والمعاهدات والمنظمات الدولية ذات الصلة بالأمن السيبراني، أطر الامتثال والمعايير: معايير وضوابط الأمن السيبراني الوطنية والدولية (مثل إطار الأمن السيبراني للقطاع المصرفي الأردني وضوابط الأمن السيبراني الصادرة عن المركز الوطني للأمن السيبراني)، HIPAA، ISO 27001، (PCI DSS، قانون الأمن السيبراني الدولي والسياسات، الاستجابة للحوادث ومتطلبات الإبلاغ، تشريعات ولوائح حماية الخصوصية والبيانات (مثل القانون العام لحماية البيانات)، تشريعات ولوائح حماية الملكية الفكرية ، المبادئ التوجيهية وأفضل الممارسات في الاتجاهات الحديثة (مثل BYOD ، وإرشادات حماية إنترنت الأشياء)، وأفضل الممارسات للمواءمة مع تشريعات وضوابط ومعايير الأمن السيبراني.
15410	**سلامة البيانات والمصادقة** **متطلب سابق: 15310** **عدد الساعات المعتمدة: 3** يوفر هذا المساق الى توفير استكشاف متعمق لسلامة البيانات والمصادقة عليها، بما في ذلك المبادئ وأفضل الممارسات لضمان دقة البيانات واكتمالها ومصداقيتها. سيغطي المقرر المواضيع التالية: نظرة عامة على تكامل البيانات والمصادقة. تقنيات تكامل البيانات بما في ذلك تكرار البيانات والمجاميع الاختبارية ورموز تصحيح الأخطاء ورموز مصادقة الرسائل (CBC– , MAC MAC)، التوقيعات الرقمية، التشفير المصدق وأشجار التجزئة. تقنيات لمصادقة، بما في ذلك تقنيات لمصادقة البيانات والمستخدمين، قوة المصادقة – مصادقة كلمات المرور، الرموز المميزة للتشفير، مصادقة القياسات الحيوية، المصادقة متعددة العوامل، وكلمات المرور لمرة واحدة والمصادقة المستندة إلى المعرفة. تقنيات هجوم كلمة المرور: هجوم القاموس، هجوم القوة الغاشمة، هجوم جدول قوس قزح، التصيد الاحتيالي، الهندسة الاجتماعية. تقنيات تخزين كلمات المرور: بما في ذلك، وظائف التجزئة المشفرة ومقاومة الاصطدام والتمليح وعدد التكرار واشتقاق المفتاح المستند إلى كلمة المرور. البروتوكولات المتقدمة على سبيل المثال لا الحصر، البراهين والمعرفة الصفرية. تحليل التحقق (تحليل التحقق الرسمي، تحليل التحقق غير الرسمي). في نهاية هذا المقرر، سيكون الطلاب قد اكتسبوا خبرة عملية في ضمان سلامة البيانات ومصداقيتها وسيكونون قادرين على تصميم وتنفيذ وتقييم حلول حماية البيانات لمختلف التطبيقات.

15411	**التحليل الرقمي والاستجابة للحوادث** **متطلب سابق: 11335** **عدد الساعات المعتمدة: 3** يعتبر هذه المقرر بمثابة مقدمة عامة في مجال التحقيقات الرقمية. ويغطي العديد من المجالات والتي تشمل فحص الملفات والأقراص والذاكرة والشبكات السلكية واللاسلكية والمتنقلة وقواعد البيانات والبرامج الضارة والبريد الإلكتروني الخ. بالإضافة إلى ذلك، يقدم المقرر للطلاب أفضل الممارسات والمعايير المتعلقة بالاستجابة للحوادث. في نهاية هذا المقرر، سيكون الطلاب قد اكتسبوا فهمًا عميقًا للطب الشرعي الرقمي والاستجابة للحوادث وسيكونون قادرين على تصميم وتنفيذ وتقييم استراتيجيات الاستجابة الفعالة للحوادث المختلفة وتقييم استراتيجيات الاستجابة الفعالة للحوادث المختلفة.
15412	**مختبر التحليل الرقمي والاستجابة للحوادث** **متطلب متزامن: 15411** **عدد الساعات المعتمدة: 1** في هذا المختبر يبدأ الطلاب ممارسة التحقيقات الرقمية في بيئة مختبر متخصص باستخدام الأدوات الأكثر استخدامًا في هذا المجال. سوف يتعلم الطلاب ممارسة أساسيات التحقيقات، والتعامل مع وسائل التخزين والأجهزة التي تحتوي على الأدلة، وكيفية جمع الأدلة والمحافظة عليها، وتطبيق أساليب التحقق من صحة الأدلة، وتقييم منهجيات التحقيقات، وإجراء تحليل الأدلة، وعمل تقارير وتقديم نتائج التحقيق الجنائي للجهات المختصة. في نهاية هذا المقرر، سيكون الطلاب قد اكتسبوا خبرة عملية في تصميم وتنفيذ الطب الشرعي الرقمي وحلول الاستجابة للحوادث لمختلف التطبيقات.
15433	**تحليل البرامج الخبيثة والهندسة العكسية** **متطلب سابق: 11335** **عدد الساعات المعتمدة: 3** سيقوم هذا المقرر بتقديم الطلاب إلى التقنيات الحديثة في تحليل البرامج الخبيثة من خلال القراءات والتحليل التفاعلي لعينات العالم الحقيقي. وتشمل الموضوعات لمحة عن نظام الحاسوب، وهندسة المعالج **X86**، ولغة التجميع (**16-bit**)، وأوضاع العنوان وأكواد الآلة، ومدخل لتحليل البرامج الخبيثة، وتحليل البرامج الخبيثة في الأجهزة الافتراضية، وتحليل البرامج الخبيثة الثابت، وتحليل البرامج الخبيثة الديناميكي، والهندسة العكسية، (لمحة عامة، تحليل **X86**، برنامج (**IDA Pro**)، التعرف على بناء الكود **C** في لغة التجميع، تحليل البرامج الخبيثة لنظام ويندوز، وتصحيح الأخطاء **X86**)، وسلوك البرامج الخبيثة، وترميز البرامج الخبيثة (التضليل والتشفير). بحلول نهاية المقرر سيكون لدى الطلاب المهارات اللازمة لتحليل البرامج الخبيثة المعاصرة باستخدام التحليل الثابت والديناميكي. سيتعلم الطلاب كيفية تحليل البرامج الخبيثة باستخدام مفاهيم الهندسة العكسية بشكل آمن وشامل. يهدف هذا التحليل إلى فهم سلوك البرامج الخبيثة وتقييم تأثيرها الأمني المحتمل.

15453	**القرصنة الأخلاقية واختبار الاختراق** **متطلب سابق: 15411** **عدد الساعات المعتمدة: 3** يغطي هذا المقرر الطرق الشائعة المستخدمة في اختبار الاختراق والقرصنة الأخلاقية لاكتشاف الأنظمة وحمايتها من الهجمات. يغطي المقرر كلاً من الجوانب النظرية والعملية للقرصنة الأخلاقية واختبار الاختراق، ويركز على تصميم وتنفيذ استراتيجيات اختبار فعالة. تشمل الموضوعات اكتشاف البصمة، الاستطلاع، طرق جمع المعلومات، كشف كلمات المرور، اختراق الشبكة (هجوم **DoS**، التنصت، الانتحال، اختطاف الجلسة)، القرصنة على الويب (هجمات حقن **SQL**، هجمات البرمجة عبر المواقع، وهجوم التزوير عبر الموقع، إلخ.)، الهندسة الاجتماعية والامتيازات المتصاعدة. في جميع الحالات، سيتعلم الطلاب كيفية كتابة التقارير وتطبيق التقنيات العلاجية. مع نهاية المقرر، سيكون الطلاب قد اكتسبوا فهمًا عميقًا للقرصنة الأخلاقية واختبار الاختراق وسيكونون قادرين على تصميم وتنفيذ وتقييم استراتيجيات الاختبار الفعالة لمختلف التطبيقات.
15483	**إدارة مخاطر أنظمة المعلومات** **متطلب سابق: 15382** **عدد الساعات المعتمدة: 3** يقدم هذا المساق مقدمة لإدارة مخاطر نظم المعلومات، بما في ذلك تحديد المخاطر، وتقييم المخاطر وتحليلها، والتهديدات الداخلية، ونماذج ومنهجيات تقييم وتقييم المخاطر، ومراقبة المخاطر. سيغطي هذا المقرر الموضوعات التالية: دورة حياة إدارة المخاطر وخطواتها ، ومنهجيات تقييم وتحليل المخاطر السيبرانية، ومنهجيات قياس وتقييم المخاطر السيبرانية، ومعايير وأطر إدارة المخاطر الإلكترونية، وعمليات إدارة المخاطر الإلكترونية عبر المستويات في المؤسسة، واقتصاديات التخفيف من المخاطر السيبرانية ونقل وقبول وتخفيف المخاطر الإلكترونية وسياسات المخاطر الإلكترونية للتقنيات وإجراءات ومعايير المخاطر والأفراد والكيانات وخصائص المنظمات التي تؤثر على المخاطر الإلكترونية والتحليل والإدارة والإبلاغ عن المخاطر الإلكترونية ونظرة عامة على استمرارية الأعمال والكوارث التعافي، بما في ذلك تحليل تأثير الأعمال، وتخطيط التعافي من الكوارث، والاختبار. مع نهاية هذا المقرر، سيكون الطلاب قد اكتسبوا فهمًا قويًا لإدارة مخاطر أنظمة المعلومات وسيكونون قادرين على تطبيق منهجيات وأطر إدارة المخاطر لإدارة المخاطر على أنظمة المعلومات في مؤسساتهم.
15490	**التدريب العملي** **متطلب سابق: انهاء 90 ساعة معتمدة** **عدد الساعات المعتمدة: 3** على الطالب أن يتدرب في مؤسسة ذات صلة بالتخصص لمدة شهرين متواصلين بدوام كامل بواقع ست ساعات يومياً. أو لمدة 3 شهور بواقع 4 ساعات يوميا. بالإضافة الى ساعات التدريب، لا يسمح للطالب الذي يتدرب بدوام غير كامل أن يسجل أكثر من 10 ساعات خلال الفصل الاول أو الفصل الثاني ولا يسمح له بالتسجيل أكثر من 4 ساعات في الفصل الصيفي. يتوقع من الطالب أن يقوم بتصميم أو إجراء تطبيق حاسوبي من ضمن تخصصه وذلك بتحليل أو تصميم أو تنفيذ برمجيات معينة تطلب منه، أو تعلم برمجيات جديدة.

15491	**مشروع التخرج (1)** **متطلب سابق: انهاء 90 ساعة معتمدة** **عدد الساعات المعتمدة: 1** يهدف مشروع التخرج إلى تطوير مهارات الطالب وقدرته على حل المسائل الواقعية ودراستها وتحليلها وتطوير البرمجيات اللازمة لحلها. ويتحقق ذلك من خلال مشروع متكامل يبرمجه الطالب ضمن فريق من الطلاب وبإشراف عضو هيئة تدريس. يطلب من الطالب إتمام أهداف المشروع وتسليم تقرير نهائي عنه. تتم مناقشة المشروع من قبل لجنة تتكون من أعضاء هيئة التدريس في البرنامج.
15492	**مشروع التخرج (2)** **متطلب سابق: 15491** **عدد الساعات المعتمدة: 2** تهدف مادة مشروع التخرج (2) الى تمثيل جميع المتطلبات التي تم التخطيط لها في مشروع التخرج (1). على الطلبة العمل ضمن مجموعات لتحقيق جميع الأهداف وفي نهاية المشروع سوف يتم انجاز نظام فعال. يجب على الطلبة اختيار جودة النظام وتوثيق ذلك.
15340	**إدارة الهوية** **متطلب سابق: 15310** **عدد الساعات المعتمدة: 3** يوفر هذا المقرر للطلاب فهماً شاملاً لمفاهيم وتقنيات وأفضل الممارسات في إدارة الهوية في سياق الأمن السيبراني. تتضمن الموضوعات: التعرف والمصادقة: الأشخاص والأجهزة، التحكم في الوصول إلى الشبكة(**NAC**) ، إدارة الوصول إلى الهوية (**IAM**)، الأدوار، نظم التعرف والمصادقة المتعددة الطرق، نظم المصادقة البيومترية، الدقة**FRR** / **FAR** ، المقاومة، الخصوصية، سهولة الاستخدام والتحمل للطرق. التحكم في الأصول المادية والمنطقية: معدات النظام، أصول الشبكة، أجهزة النسخ الاحتياطي / التخزين، التحكم في الوصول القائم على القواعد(**RAC**) ، التحكم القائم على الأدوار(**RBAC**) ، طرق تتبع المخزون، طرق إنشاء الهوية. الهوية كخدمة(**IaaS**) ، خدمات الهوية الطرف الثالث، هجمات وتدابير التخفيف للتحكم في الوصول: كلمة المرور، قاموس، هجمات القوة القسرية، التزييف، المصادقة متعددة العوامل، سياسة كلمة المرور القوية، ملفات كلمة المرور الآمنة وتقييد الوصول إلى الأنظمة. بنهاية المقرر، سيكون الطلاب قد اكتسبوا فهمًا جيدًا لمبادئ إدارة الهوية والممارسات، مما يتيح لهم تصميم وتنفيذ وإدارة حلول إدارة الهوية الفعالة للتطبيقات المختلفة.

15371	**الجرائم السيبرانية** **متطلب سابق: 15310** **عدد الساعات المعتمدة: 3** يهدف هذا المساق إلى تزويد الطلاب بفهم شامل لمختلف جرائم الإنترنت والانتهاكات السائدة في العالم الرقمي. من خلال استكشاف تأثيرها على الأفراد والمنظمات والمجتمع. يجب تضمين الموضوعات التالية في هذا المقرر: أنواع جرائم الإنترنت: (الاختراقات، الفدية، التجسس، سرقة الملكية الفكرية، الاحتيال، الابتزاز، تعطيل الخدمات، تسريب البيانات، تدمير البيانات، تزوير البيانات)، التحرش الإلكتروني والمفترسين، التنمر الإلكتروني، سرقة الهوية، جرائم الإنترنت المعاونة، الإرهاب الإلكتروني، وقوانين جرائم الإنترنت: القوانين الوطنية، القوانين الدولية، المعاهدات. بعد إكمال هذا المقرر، سيكون الطلاب قادرين على تحديد جرائم الإنترنت، فهم تأثيرها المجتمعي، وتقييم القوانين ذات الصلة، ووضع استراتيجيات لمعالجتها.
15383	**تكنولوجيا البلوك شين** **متطلب سابق: 15310** **عدد الساعات المعتمدة: 3** يقدم هذا المساق استكشافًا شاملاً لتكنولوجيا البلوك شين وتطبيقاتها المختلفة. وكذلك أساسيات تكنولوجيا الدفاتر الموزعة وآليات الاتفاق وتقنيات المصادقة والبروتوكولات ذات الصلة. يساعد هذا المساقة الطلاب على فهم لأنظمة البلوك شين مثل بتكوين وإيثريوم ومقدمة إلى منصات البلوك شين البديلة. من خلال هذه المساق، سيدرس الطلاب التطبيقات الحقيقية لتكنولوجيا البلوك شين، بما في ذلك العملات الرقمية وإدارة سلاسل الإمداد وسيناريوهات **B2B / B2C / C2C**. بالإضافة إلى ذلك، سيحصل الطلاب على تجربة عملية في بناء ونشر العقود الذكية والتطبيقات الموزعة.
15413	**التحقيقات الرقمية المتقدم** **متطلب سابق: 15411** **عدد الساعات المعتمدة: 3** يقدم هذا المساق المنهجية والإجراءات المرتبطة بتحليل التحقيقات الرقمية للحوادث التي تشمل أجهزة متصلة بالإنترنت، أو متعلقة بأجهزة الحاسوب، أو المتعلقة بالشبكات والأجهزة الخلوية. يشمل المساق المواضيع التالية: تكوين نظام تشغيل آمن باستخدام الأوامر المكتوبة وأدوات الواجهات الرسومية. يتم التركيز على هيكلية أنظمة الملفات في أنظمة التشغيل، ونقاط الضعف الأمنية فيها، وأمن المستخدم، وطرق تحصين أنظمة التشغيل واختراقها، وطرق استعادة البيانات والملفات المطلوبة للتحقيقات الرقمية. الموضوعات الحصول على بيانات الشبكة، وتحليل الأدلة الجنائية للشبكات، وسجلات الأحداث و حركة مرور البيانات في الشبكة، والحصول على البيانات وتحليلها، وإدارة أنظمة كشف / منع التسلل (**IDS / IPS**) ، وإدارة الحوادث الأمنية ونظم إدارة الحوادث (**SIEM**) ، إلخ. على تكنولوجيا الأجهزة المحمولة والأجهزة المحمولة والشبكات الخلوية ثم على عمليات وأساليب وتقنيات التحقيقات الرقمية للهواتف والأجهزة المتنقلة.

15420	**امن الشبكات اللاسلكية والمتنقلة** **متطلب سابق: 15220** **عدد الساعات المعتمدة: 3** يركز هذا المقرر على التحديات الأمنية والمتطلبات في مجال الاتصالات المتنقلة وشبكات الاتصال اللاسلكية وشبكات الهاتف المحمول. تشمل الموضوعات: أساسيات الأمان اللاسلكي والمتنقل، بروتوكولات الأمان لشبكات الاتصال اللاسلكية مثل (**WEP, WPA, WPA2, WPA3**). الأمان على مستوى التطبيق في شبكات الاتصال اللاسلكية: تطبيقات **WLANs**، التهديدات اللاسلكية، بعض ثغرات الأمان وطرق الهجوم عبر شبكات**WLANs** ، الأمان لتطبيقات (**1G Wi-Fi**)، الأمان لتطبيقات (**2G Wi-Fi**)، ومخططات الأمان الحديثة لتطبيقات (**Wi-Fi**). الأمان في تقنيات (**Bluetooth, NFC and RFID**) .أمان شبكات الاتصال المحمولة، بما في ذلك آليات الأمان لشبكات (**GSM, CDMA, 3G, 4G, 5G**)، وكذلك التحديات والثغرات المرتبطة بهذه التقنيات. بنهاية المقرر، سيكون الطلاب قد اكتسبوا المعرفة والمهارات اللازمة لتأمين الأجهزة المتنقلة وشبكات الاتصال اللاسلكية بفعالية في مختلف البيئات.
15422	**أمن الوسائط المتعددة** **متطلب سابق: 11213** **عدد الساعات المعتمدة: 3** امن وحماية الوسائط المتعددة: هو مادة شاملة تغطي العديد من التقنيات والخوارزميات المستخدمة لتأمين المحتوى المتعدد الوسائط من الوصول غير المصرح به والاستخدام والتعديل أو التوزيع. سيتعلم الطلاب عن التقنيات العملية المتعلقة بالتشفير والواترمارك والستيغانوجرافي وإدارة الحقوق الرقمية والتهديدات الجديدة مثل الـ **DeepFake**. تشمل الدورة أيضًا التحليل المتعدد الوسائط(**Multimedia forensics**) ، والذي يتضمن استخدام تقنيات التحليل الرقمي لتحليل البيانات المتعددة الوسائط وتحديد صحتها ونزاهتها ومصدرها. من خلال الدورة، سيتطور لدى الطلاب فهم شامل لمبادئ وممارسات أمن المحتوى المتعدد الوسائط وسيتعلمون المهارات اللازمة لتطوير تطبيقات متعددة الوسائط آمنة، واستكشاف التقنيات والأدوات الجديدة لحماية المحتوى المتعدد الوسائط.
15423	**أمن الحوسبة السحابة** **متطلب سابق: 15321** **عدد الساعات المعتمدة: 3** يقدم هذا المساق للطلاب فهماً شاملاً لتحديات الأمان المرتبطة ببيئات الحوسبة السحابية. تتضمن الموضوعات: منصات الافتراضية، نماذج الحوسبة السحابية (**IaaS, PaaS, SaaS, DaaS**)، موفري خدمات السحابة وعروضهم الأمنية، نماذج تنفيذ السحابة (العامة، الخاصة، المختلطة، المجتمعية)، الهايبرفايزر وتنفيذات الحوسبة السحابية، تقييم المخاطر وإدارتها في بيئات السحابة، تشفير البيانات وإدارة المفاتيح، آليات التحكم الآمنة في الوصول، تأمين البيئات الافتراضية، معايير وشهادات أمان السحابة، التدقيق والرصد في السحابة، استجابة الحوادث وتخطيط استعادة الكوارث، والقضايا القانونية والخصوصية والامتثال التنظيمي في السحابة. بنهاية المساق، سيكون الطلاب قد اكتسبوا فهماً ثابتاً لمفاهيم وأفضل الممارسات المتعلقة بأمان الحوسبة السحابية.

15425	**برمجة الشبكات** **متطلب سابق: 11335** **عدد الساعات المعتمدة: 3** يقدم هذا المقرر الدراسي للطلاب المفاهيم والتقنيات الأساسية لبرمجة الشبكات. تتضمن الموضوعات: بروتوكولات الشبكة والهياكل، برمجة المقابس(**sockets**) ، والاتصالات المعلوماتية، وتطوير تطبيقات الشبكة. بروتوكولات **TCP / IP** و**UDP**، برمجة المقابس بلغات مختلفة مثل (**C, Java, Python**)، وترميز البيانات وتسلسلها، وأنماط تصميم تطبيقات الشبكة. سيستكشف الطلاب أيضًا أمثلة واقعية على تطبيقات الشبكة، مثل خوادم الدردشة وبرامج نقل الملفات وخدمات الويب. بنهاية المقرر، سيكون الطلاب قادرين على تصميم وتطوير وتنفيذ تطبيقات الشبكة الآمنة والقوية بشكل فعال.
15434	**أمن إنترنت الأشياء** **متطلب سابق: 15321** **عدد الساعات المعتمدة: 3** إنترنت الأشياء (**IoT**) هي إحدى المجالات الجديدة سريعة التطور التي تؤدي الى تغيير كيفية تفاعلنا مع التكنولوجيا. يركز هذا المساق على التكنولوجيات الأساسية التي تدعم شبكات**IoT**، بما في ذلك الحساسات والأنظمة المضمنة والحوسبة السحابية وبروتوكولات الاتصال اللاسلكية المستخدمة في شبكاتانتنت الأشياء (بما في ذلك الواي فاي، البلوتوث، زيكبي، الشبكات الخلوية). سيوفر هذا المساق أيضًا فهمًا عميقًا للمخاطر الأمنية المرتبطة بأجهزة **IoT** وكيفية التخفيف منها. في هذا المساق، ستتعلم عن الطبقات المختلفة لأمن **IoT** ، بما في ذلك الأمن الفيزيائي والشبكات والتطبيقات والبيانات، والتحديات الأمنية المختلفة المرتبطة بشبكات **IoT**، مثل مصادقة الأجهزة وخصوصية البيانات وسلامة البيانات. سيتعلم الطلاب أيضًا عن التهديدات الشائعة التي تستهدف أجهزة**IoT**، مثل البرامج الضارة والشبكات الروبوتية وهجمات إنكار الخدمة الموزعة (**DDoS**).بعد إكمال هذا المساق، سيمتلك الطلاب فهمًا قويًا لتكنولوجيا **IoT** والتحديات الأمنية المرتبطة بشبكات**IoT**، والمهارات اللازمة لتأمين أجهزة **IoT** والشبكات ضد التهديدات السيبرانية.
15435	**أمن العتاد المادي** **متطلب سابق: 15310** **عدد الساعات المعتمدة: 3** الأمن الفيزيائي للأجهزة هو جانب مهم من جوانب الأمن السيبراني الذي يتعامل مع حماية المكونات الفعلية لنظم الحوسبة من الوصول غير المصرح به والتلاعب والاستغلال. يغطي هذا المساق المفاهيم الأساسية والتقنيات والتحديات الخاصة بأمن الأجهزة. سيركز هذا المساق على الموضوعات التالية: مقدمة حول أمن الأجهزة وأهميته، نماذج التهديدات ومتجهات الهجوم لأنظمة الأجهزة، وآليات أمن الأجهزة وإجراءات الدفاع، مثل التشفير ومراقبة الوصول والحمايات الفعلية، والحوسبة الموثوقة وعمليات التشغيل الآمنة، وهجمات القنوات الجانبية والدفاعات المضادة، وتقنيات الهندسة العكسية والتلاعب، ومنهجيات اختبار وتقييم أمن الأجهزة، ودراسات الحالة لانتهاكات أمن الأجهزة في العالم الحقيقي وأثرها. بعد إكمال هذا المساق، سيكتسب الطلاب فهما شاملا لمفاهيم وتقنيات أمن الأجهزة ويتمتعون بالمهارات اللازمة لتصميم وتقييم والدفاع عن أنظمة الأجهزة ضد التهديدات الأمنية.

15443	**الهندسة الاجتماعية والعوامل البشرية** **متطلب سابق: 15110** **عدد الساعات المعتمدة: 3** يستكشف هذا المقرر دور العوامل البشرية والهندسة الاجتماعية في مجال الأمن السيبراني، مع التركيز على الجوانب النفسية والاجتماعية والسلوكية التي تسهم في نجاح الهجمات الإلكترونية. تشمل الموضوعات: العوامل البشرية في الأمن السيبراني. أنواع هجمات الهندسة الاجتماعية (هجمات التصيد الإلكتروني والتصيد الإلكتروني الموجه، الاختراق الجسدي / التنكر، التصيد الهاتفي (التصيد عبر الهاتف)، والاختراق عبر البريد الإلكتروني والتحريض). علم النفس لهجمات الهندسة الاجتماعية (التفكير التنافسي، كيف تؤثر الاستجابات العاطفية على اتخاذ القرارات، التحيزات المعرفية للمخاطر والمكافآت، وبناء الثقة). تضليل المستخدمين) تزييف مرسلي الرسائل، عناوين **URL** المضللة، كيف يحكم المستخدمون ويثقون بصفحات الويب ورسائل البريد الإلكتروني، بالإضافة إلى سلوكيات المستخدمين مع التصيد الإلكتروني وتحذيرات المتصفح الأخرى .(كشف وتخفيف هجمات الهندسة الاجتماعية. بنهاية المادة، سيتمكن الطلاب من تحديد وتحليل وتخفيف تهديدات الهندسة الاجتماعية بفعالية، مما يعزز موقف الأمان الشامل للمنظمات.
15455	**أمن التجارة الالكترونية** **متطلب سابق: 15261** **عدد الساعات المعتمدة: 3** أمن التجارة الإلكترونية هو مساق يركز على حماية التجارة الإلكترونية وتأمينها من الوصول غير المصرح به والاختراق وسرقة البيانات والاحتيال الإلكتروني. يغطي هذا المساق موضوعات مثل الأمن السيبراني، والتشفير، وأمن البرمجيات، والحماية من الفيروسات والبرامج الخبيثة، والتعرف على الاختراقات ومعالجتها، بالإضافة إلى دراسة حالات الاحتيال الإلكتروني والتدابير الوقائية المتخذة ضدها. كما يستكشف المساق أيضًا أساليب تأمين الشبكات والتطبيقات وحماية البيانات الحساسة والملكية الفكرية في بيئة التجارة الإلكترونية. يهدف هذا المساق إلى تزويد الطلاب بالمهارات والمعرفة اللازمة لتأمين بيئة التجارة الإلكترونية والمحافظة على خصوصية المستخدمين وأمانهم في الدفعات الإلكترونية.
15485	**المرونة السيبرانية واستمرارية الأعمال** **متطلب سابق: 15382** **عدد الساعات المعتمدة: 3** في هذا المقرر، سيتعلم الطلاب المبادئ وأفضل الممارسات لضمان المرونة السيبرانية واستمرارية الأعمال في مواجهة التهديدات الإلكترونية المختلفة والحوادث. تتضمن الموضوعات: فهم العلاقة بين الأمن السيبراني واستمرارية الأعمال، التخطيط لاستجابة الحوادث (توقع، كشف وتقليل)، تخطيط استعادة الأعمال بعد الكوارث، الاتصال في أوقات الأزمات، وإدارة العنصر البشري في الحوادث السيبرانية، استمرارية الأعمال (التخطيط البديل، استجابة الحوادث، الاستجابة للطوارئ، النسخ الاحتياطي والاستعادة). تنفيذ استراتيجيات النسخ الاحتياطي الفعّالة، وأهمية اختبار وصقل هذه الخطط بانتظام. بنهاية المقرر، سيكون لدى الطلاب المعرفة والمهارات اللازمة لتطوير وتنفيذ وصيانة استراتيجيات شاملة للمرونة السيبرانية واستمرارية الأعمال، مما يقلل بفعالية من التوقف عن العمل ويقلل من تأثير الحوادث السيبرانية على عمليات المنظمة.

15493	**مواضيع مختارة في الامن السيبراني (1)** **متطلب سابق: موافقة القسم** **عدد الساعات المعتمدة: 3** يهدف هذا المساق إلى إدخال موضوعات جديدة في أحد فروع الأمن السيبراني. يتم بعناية اختيار مواضيع في مجال الأمن السيبراني أكثر حداثة والمرتبطة بالمسار المهني للطالب ويجب أن يكون الطالب قد درس المتطلبات التي تمكنه من فهم هذه المواضيع. يمكن أن يحتوي هذا المقرر على تقنيات حديثة أو مواضيع متقدمة سبق للطالب دراستها بصورة مبسطة. يقرر القسم الموضوع ومتطلباته.
15494	**مواضيع مختارة في الامن السيبراني (2)** **متطلب سابق: موافقة القسم** **عدد الساعات المعتمدة: 3** يهدف هذا المساق إلى إدخال موضوعات جديدة في أحد فروع الأمن السيبراني. يتم بعناية اختيار مواضيع في مجال الأمن السيبراني أكثر حداثة والمرتبطة بالمسار المهني للطالب ويجب أن يكون الطالب قد درس المتطلبات التي تمكنه من فهم هذه المواضيع. يمكن أن يحتوي هذا المقرر على تقنيات حديثة أو مواضيع متقدمة سبق للطالب دراستها بصورة مبسطة. يقرر القسم الموضوع ومتطلباته.