

## جامعة الزرقاء

### كلية تكنولوجيا المعلومات

#### وصف المواد لبرنامج الماجستير في الامن السيبراني

اسم المساق	عدد الساعات	التوصيف
منهجية البحث العلمي	3	يتناول هذا المساق البحث النوعي والكمي، ومناهج البحث العلمي، والتصميم التجريبي وأخذ العينات، والقياس، والتحليل. كما ويتطرق إلى أخلاقيات البحث العلمي، وكيفية كتابة البحوث العلمية والنشر في المجالات العلمية، ومكونات الورقة البحثية. ويقدم هذا المساق تفصيلاً عن كيفية كتابة الرسائل الجامعية واجراء التجارب وكتابة النتائج والتقارير.
سلسلة الكتل	3	يقدم هذا المساق نظرة عامة شاملة على البلوكشين، بما في ذلك مبادئها وتطبيقاتها وتحدياتها. خلال المساق، سيستكشف الطلاب المفاهيم الأساسية للبلوكشين، بما في ذلك الشبكات اللامركزية وتكنولوجيا ملف الحسابات الموزع وبروتوكولات التشفير وآليات الإجماع والعقود الذكية. سوف يتعمقون في تطوير البلوكشين ويكتسبون رؤى حول تطورها وحالتها الحالية. ستوفر التدريبات والمشاريع العملية خبرة عملية في تطوير البلوكشين، و سوف يكون لدى الطلاب فهم قوي للبلوكشين والقدرة على تطوير ونشر الحلول المستندة إلى البلوكشين. يعد هذا المساق الطلاب للمساهمة في مجال التطور السريع لتكنولوجيا البلوكشين.
أمن الشبكات المتقدمة	3	يتناول هذا المساق القضايا الرئيسية في اتصالات البيانات وأمن الشبكات وكيفية الوصول إلى المعلومات، واهم المواضيع التي سيتم تغطيتها في هذا المساق تشمل تعريف الأمان وأمن الشبكة والتوقيعات الرقمية وأمان IP والمقبس الأمان طبقة، كشف التنسل، المصادقة، جدران الحماية، رفض الخدمة، البريد العشوائي، فيروسات البريد الإلكتروني، التصيد الاحتيالي، ونظرة عامة على العديد من الهجمات التي تتعرض لها الشبكات والطرق المناسبة للتعامل معها ومنعها.
مواضيع متقدمة في القرصنة الأخلاقية	3	يلقي هذا المساق الضوء على أدوات القرصنة الأخلاقية لتطوير المهارات والتقنيات لتحديد نقاط ضعف المضيف والشبكة. كما ويوفر المساق الفهم لنطاق اختبارات الاختراق ومسؤوليات إجراء هذه الاختبارات باتباع مدونة أخلاقية صارمة. إضافة إلى استخدام مجموعة من أدوات البرمجيات الحديثة لأداء مهام اختبار الاختراق المختلفة على مزودات الخدمة، وكيفية تنفيذ آليات دفاع مناسبة للتخفيف من المشكلات المحددة ومعالجتها.
مواضيع متقدمة في التشفير	3	يعرض هذا المساق طرق وتقنيات التشفير وفك التشفير. ويتضمن شرحاً عن المفاتيح العامة والخاصة، والبروتوكولات، ومولدات الأرقام، والتوقيعات الرقمية، وأوجه التشفير الأخرى. بالإضافة إلى ذلك يتم تسليط الضوء على الدور الذي تلعبه الأخلاقيات وخصوصية المعلومات عند تطبيق الأمان على الأنظمة العامة ومحتوى البريد

الإلكتروني بالإضافة إلى مستويات أعلى من الأمان للشركات المملوكة والمعلومات الحكومية المصنفة.		
يغطي هذا المساق طرق وإجراءات تحديد واستعادة البيانات الرقمية التالفة أو المحذوفة، والوصول إلى معلومات التتبع، مثل سجل الويب، وملفات تعريف الارتباط، وذاكرة التخزين المؤقت. كما ويلقي الضوء على كيفية مصدر الهجمات على شبكة الإنترنت. كما ويهتم هذا المساق بتحديد نقاط الضعف في النظام، ومنافذ الاتصال، وطرق التشفير. علاوة على ذلك يسلط هذا المساق الضوء على موضوع مراقبة الحوادث والاستجابة لها.	3	تحقيقات الأدلة الرقمية
يهتم هذا المساق في دراسة القوانين التي ترتبط بالفضاء السيبراني. حيث سيتم دراسة القوانين والأنظمة التي تحكم التعامل مع المعلومات وتراسلها في الفضاء السيبراني. كما سيتم دراسة الجرائم الإلكترونية بمختلف أنواعها مثل الخصوصية وانتحال الشخصية والتنصل وبالأخص الجرائم المتعلقة بالتجارة الإلكترونية. كما سيتم دراسة القوانين التي تحكم هذه الجرائم وكيفية تحليلها والأدلة الرقمية المرتبطة فيها بصورة قانونية.	3	الجرائم والقوانين السيبرانية
يحتوي هذا المساق على مراجعة تفصيلية وتحليلاً لإطار عمل إدارة المخاطر ( Risk Management Framework) والمكون من ست خطوات باستخدام المنشور الخاص للمعهد الوطني للمعايير والتكنولوجيا (NIST) 800-53 (Special Publication) والذي يتضمن ضوابط الأمان والخصوصية لأنظمة المعلومات والمنظمات. ويتضمن هذا المساق عملية تحليل المخاطر وتصنيف المخاطر السيبرانية لأنظمة المعلومات، وتطبيق الضوابط لتقليل المخاطر السيبرانية لإدارة المعلومات. كما يقدم نظرة عامة متعمقة لكل خطوة من خطوات إطار العمل RMF على طول مسار إطار العمل بالإضافة إلى منهجية مراقبة أنظمة تكنولوجيا المعلومات.	3	إدارة مخاطر الأمن السيبراني
يتناول هذا المساق القضايا الرئيسية في الأمن اللاسلكي وكيفية تقييم المخاطر الأمنية في الشبكات اللاسلكية، وأهم المواضيع التي سيتم تغطيتها في هذا المساق تشمل أهم الأدوات والاتجاهات والتقنيات الخاصة بالأمن اللاسلكي والإلمام في إعداد أنظمة منع التطفل اللاسلكي (WISPS) وكيفية تصميم بنية أمان الشبكة. ويتضمن هذا المساق فهم التكنولوجيا والحلول الأمنية لشبكة WLAN، التعرف على تقنيات المصادقة مثل WPA / WPA2 Personal و Enterprise وفهم مصادقة IEEE 802.11 وإدارة المفاتيح (AKM)، كما سيتم تعلم كيفية تطبيق سياسات أمان شبكة WLAN وممارسات التدقيق وكيفية تأمين نقاط نهاية شبكة WLAN المحمولة وإدارة وتشغيل شبكة WLAN بكفاءة.	3	أمن الشبكات اللاسلكية والأنظمة المحمولة
يتطرق هذا المساق إلى مفهوم وعملية نمذجة التهديد كعامل تمكين رئيسي لهندسة أمان فعال ومناسب لأصول البرامج والمعلومات. تشمل موضوعات هذا المساق مراجعة متعمقة لأنواع مختلفة من التهديدات ضد البرامج. كما ويقدم هذا البرنامج أساسيات بناء برامج أمانة تمنع الثغرات الأمنية التي يستغلها المتسللون. تشمل الموضوعات التي يتم تناولها Buffer Overflow، والإدخال غير المُتحقق من صحته، وظروف السباق، ومشكلات التحكم في الوصول، ونقاط ضعف المصادقة أو التفويض، والتجزئة (hashing)، وممارسات الأمان الأخرى. كما ويلقي الضوء على أفضل الممارسات	3	تطوير البرمجيات الأمانة

<p>لتجنب معظم الثغرات الأمنية، وسمات الأمان للعديد من لغات البرمجة مثل C و ++ C و # C و Java و Python و PHP و Ruby.</p>		
<p>يقدم هذا المساق كيفية فحص الطرق المختلفة المستخدمة لتهديد الأنظمة السيبرانية مثل الفيروسات، والانتحال، والحرمان من الخدمة، والتصيد، وروبوتات التجسس، والرسائل الإلكترونية المزعجة، ومواقع مزيفة، والتنصت عبر الشبكات اللاسلكية. كما ويتطرق إلى الطرق المختلفة التي يستخدمها المخترقون في الوصول إلى البيانات الوطنية أو المملوكة للشركات أو الشخصية، والخسارة المتزايدة للخصوصية على الشبكات الاجتماعية. كما ويقدم هذا المساق تقنيات وأبحاث متقدمة في كشف التسلل والدفاع الشبكي، وتحليل حركة مرور الشبكة، وتحليل التسلل، وتقنيات التعلم الآلي للكشف عن التسلل، واستخراج البيانات لاكتشاف التسلل، والتحديات المستمرة المتقدمة.</p>	3	<p><b>انظمة اكتشاف الاختراق الذكية</b></p>
<p>يركز هذا المساق على التقنيات التي توفر خدمات الأمان لشبكة الويب. كما ويقدم مجموعة من الإجراءات والممارسات والتقنيات لحماية خوادم الويب ومستخدمي الويب والمؤسسات المحيطة بهم. وكما ويقوم بمناقشة وفهم واستخدام تقنيات الأمان المختلفة لشبكة الويب العالمية (WWW) وكيفية استخدام هذه التقنيات لتأمين تطبيقات WWW وتطبيقات التجارة الإلكترونية.</p>	3	<p><b>أمن التجارة الإلكترونية</b></p>
<p>يعرض هذا المساق استراتيجيات أمن المعلومات التي تدعم الأهداف والغايات التنظيمية، وتتوافق مع المتطلبات القانونية والتنظيمية المعمول بها، والتي يتم تنفيذها من خلال السياسات والضوابط الداخلية من خلال توفير الإشراف على تخفيف المخاطر. كما ويتطرق هذا المساق إلى الهيكل التنظيمي لبناء أطر تقنية المعلومات، والاستراتيجية والجوانب التكنولوجية لحوكمة تكنولوجيا المعلومات والمعرفة الأساسية حول إدارة أنواع مختلفة من المعلومات. ويقدم هذا المساق دراسة عن مخاطر الإنترنت ودراسة حول الحوكمة مع التركيز على كل من هياكل الرقابة الداخلية والتفاعل على مستوى مجلس الإدارة.</p>	3	<p><b>حوكمة الأمان السيبراني</b></p>
<p>يقدم هذا المساق تقنيات التعلم الآلي واستخراج البيانات. كما ويركز هذا المساق على استخدام الأساليب التطبيقية والأدوات البرمجية لاكتشاف الأنماط المخفية أو تحديد الحالات الشاذة في البيانات المتولدة في شبكات تكنولوجيا المعلومات الحديثة.</p>	3	<p><b>تعلم الآلة</b></p>
<p>يحتوي هذا المساق على النظرية والممارسة الفضلى في تدقيق نظم المعلومات، ويلقي الضوء على دور مدقق نظم المعلومات في تطوير النظم، وكيفية تحديد ضوابط أنظمة الحاسوب. كما ويتطرق هذا المساق إلى آلية توفير أساسيات تقييم عمليات ومنتجات مشروع هندسة البرمجيات للامتثال لمجموعة محددة من المعايير. علاوة على ذلك، يقدم هذا المساق كيفية توفير معلومات مفيدة لأي شخص يحتاج إلى تقديم تقييم مستقل للامتثال</p>	3	<p><b>التدقيق الرقمي</b></p>

		لمجموعة من العمليات والمعايير والمتطلبات المحددة.
	3	هندسة البرمجيات المتقدمة
يقدم هذا المساق كيفية بناء مشروع برمجي وإدارته بشكل احترافي، بالإضافة إلى كيفية وضع خطة مع جدول زمني للمنتجات النهائية، ونظام تتبع لمراقبة عملية بناء المشروع، وتقييم إدارة المخاطر.	3	إدارة مشاريع البرمجيات
	3	الحوسبة السحابية
	3	مواضيع متقدمة في تكنولوجيا المعلومات
يتناول هذا المساق التطورات التقنية في مجال الأمن السيبراني وأمن شبكات وأنظمة الكمبيوتر والتي لا تغطيها المساقات الأخرى في برنامج ماجستير الأمن السيبراني. قد تتغير الموضوعات من سنة إلى أخرى بناءً على مستجدات الاتجاهات الحالية في هذا المجال.	3	مواضيع خاصة في الأمن السيبراني
يقوم الطالب في هذا المقرر بإجراء بحث في أحد موضوعات الأمن السيبراني.	3	مشروع بحث