جامعة اليرموك

مركز الملكة رانيا للدراسات الأردنية وخدمة المجتمع

الخطة الدراسية للدبلوم التدريبي (المهني) في تخصص:

الأمن السيبراني

رقم المساق	اسم المساق	الساعات النظرية	الساعات العملية	الهدف من المساق	المحتوى
1	مقدمة في الأمن السيبراني	15	15	تقديم أساسيات الأمن السيبراني وأهمية حماية المعلومات على الإنترنت.	- تعريف الأمن السيبراني وأهدافه الأساسية - أهمية حماية المعلومات في العصر الرقمي - المكونات الأساسية لنظام الأمن السيبراني - التهديدات الأمنية الشائعة وكيفية الوقاية منها - المبادئ الأساسية لحماية الشبكات والأنظمة من الهجمات.
2	أنواع الهجمات السيبرانية	15	15	التعرف على الأنواع المختلفة للهجمات السيبرانية وكيفية التصدي لها.	- تصنيف الهجمات السيبرانية: مثل الهجمات المباشرة، والفيروسات، والهجمات الاحتيالية - الهجمات الإلكترونية الشائعة مثل DDoS ، Phishing، Ransomware - تقنيات الحماية من الهجمات السبرانية - كيفية اكتشاف الهجمات السيبرانية والرد عليها - تقنيات الوقاية من الهجمات المتقدمة.

رقم المساق	اسم المساق	الساعات النظرية	الساعات العملية	الهدف من المساق	المحتوى
3	حماية الشبكات	18	12	تعلم كيفية حماية الشبكات من الهجمات السيبرانية والتقنيات المتقدمة في الحماية.	- مفهوم حماية الشبكات وأهميته في الأمن السيبراني. - أدوات وتقنيات حماية الشبكات (VPN ،Firewall) - مراقبة الشبكات للكشف عن الأنشطة المشبوهة - تأمين الشبكات ضد الوصول غير المصرح به - استراتيجيات تقسيم الشبكة وتعزيز الأمن في بيئات العمل المختلفة.
4	التشفير وأمن البيانات	18	12	تعلم تقنيات التشفير وكيفية حماية البيانات الحساسة أثناء النقل والتخزين.	- مفهوم التشفير وأنواعه (التشفير المتماثل وغير المتماثل - استخدام التشفير لحماية البيانات أثناء التخزين والنقل - تقنيات التوقيع الرقمي والمصادقة باستخدام التشفير - أفضل الممارسات لتطبيق التشفير في بيئات العمل - إدارة مفاتيح التشفير وحمايتها من السرقة.

رقم المساق	اسم المساق	الساعات النظرية	الساعات العملية	الهدف من المساق	المحتوى
5	إدارة الثغرات والتهديدات الأمنية	20	10	تعلم كيفية التعرف على الثغرات الأمنية في النظام وكيفية معالجتها باستخدام أدوات الفحص والتحليل.	- كيفية تحديد وتقييم الثغرات الأمنية في النظام - استراتيجيات إدارة الثغرات بشكل فعال - تطبيق أدوات مسح الثغرات والتأكد من تغطية الثغرات في البرمجيات - تقييم تهديدات الأمان وكيفية مواجهتها - تطوير سياسة أمنية لمواكبة تهديدات الأمن السيبراني المستمرة.
6	أمن التطبيقات البرمجية	15	15	تعلم كيفية حماية التطبيقات البرمجية من الثغرات والهجمات عبر تطبيق أفضل ممارسات الأمان.	- فهم أساسيات أمن التطبيقات وأهميته - تقنيات تحسين الأمان في مراحل تطوير البرمجيات - تقنيات اختبار اختراق التطبيقات للبحث عن الثغرات - استراتيجيات حماية التطبيقات ضد الهجمات السيبرانية - استخدام أدوات التحقق من الأمان في تطبيقات البرمجيات.

رقم المساق	اسم المساق	الساعات النظرية	الساعات العملية	الهدف من المساق	المحتوى
7	الأمن في بيئات السحابة (Cloud Security)	18	12	تعلم كيفية تأمين بيئات الحوسبة السحابية وحمايتها من التهديدات والاختراقات.	- مفاهيم الأمان في السحابة وحمايتها - التحديات الأمنية في بيئات السحابة العامة والخاصة - تقنيات تأمين البيانات المخزنة في السحابة - استراتيجيات التحكم في الوصول وحمايته في بيئات السحابة - أفضل الممارسات لضمان الأمان في خدمات السحابة مثل AWS وAzure
8	الحماية ضد البرمجيات الخبيثة	15	15	تعلم كيفية اكتشاف والتصدي للبرمجيات الخبيثة مثل الفيروسات والديدان وأحصنة طروادة.	- التعريف بالبرمجيات الخبيثة (فيروسات، برامج تجسس، Ransomware) - تقنيات الكشف عن البرمجيات الخبيثة - أدوات الحماية والتصدي للبرمجيات الخبيثة - كيفية الوقاية من الهجمات باستخدام البرمجيات الخبيثة - إجراءات العزل والاستجابة عند اكتشاف البرمجيات الخبيثة.

رقم المساق	اسم المساق	الساعات النظرية	الساعات العملية	الهدف من المساق	المحتوى
9	استجابة الحوادث والتحقيقات الجنائية الإلكترونية	20	10	تعلم كيفية الاستجابة لحوادث الأمان الجنائي وإجراء التحقيقات الرقمية في الحالات الطارئة.	- مراحل استجابة الحوادث السيبرانية (الكشف، التقييم، التفاعل) - كيفية إجراء التحقيقات الجنائية الإلكترونية - جمع الأدلة الرقمية وتحليلها بشكل قانوني - التعامل مع الحوادث بشكل منظم لتقليل الأضرار - تقنيات التوثيق والتقارير الخاصة بالحوادث الأمنية.
10	إدارة الأمان السيبراني في المؤسسات	18	12	تعلم كيفية إدارة وتطبيق استراتيجيات الأمان السيبراني في بيئات العمل المؤسسية.	- استراتيجيات إدارة الأمان في المؤسسات والشركات - أهمية وجود سياسة أمنية شاملة للمؤسسة - تكامل أنظمة الأمان المختلفة في المؤسسة - إدارة الفرق المتخصصة في الأمن السيبراني - تطبيق أفضل الممارسات لضمان استمرارية الأمان على المدى الطويل.