جامعة فيلادلفيا
كلية تكنولوجيا المعلومات

برنامج
الدبلوم التدريبي التطبيقي في

الأمن السيبراني

Applied Training Diploma in Cyber Security

شباط 2021

الدبلوم التدريبي التطبيقي في الأمن السيبراني

Applied Training Diploma in Cyber Security

مقدمة عن البرنامج

أصبحت حماية وأمن المعلومات ضرورة ملحة بالنسبة للأفراد والمؤسسات على شتى أنواعها حيث ينبغي لهم امتلاك المعرفة بالطرق التي تحميهم من القرصنة التي تهدد أمن معلوماتهم، ومع انتشار الوسائل التقنية لمعالجة وتخزين البيانات وتداولها وتبادلها والتفاعل معها عبر الإنترنت وشبكات المعلومات، أصبح أمن الفضاء الإلكتروني أو ما يسمى بـ «الأمن السيبراني» توجهاً عالمياً لحماية الأنظمة والأجهزة والبيانات الإلكترونية في شتى منظمات الأعمال والبيانات.

يعتبر مجال الأمن السيبراني من أكثر المجالات حيوية في قطاع تقنية المعلومات حيث يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من التهديدات المحتملة، وتحديد طرق الاختراق الحديثة وتفاديها، وتقييم الثغرات ونقاط الضعف في النظم والشبكات الحاسوبية، ومعالجة الثغرات المؤدية إلى الاختراقات الأمنية، واستخدام وتطوير برمجيات التشفير وأمن المعلومات.

يوفر برنامج الدبلوم التدريبي التطبيقي في الأمن السيبراني من الناحية التقنية الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. ومن الناحية القانونية، فإن أمن المعلومات يعد محل دراسات وتدابير قانونية لحماية سرية وسلامة المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهو هدف تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها كجرائم الإنترنت والجرائم الالكترونية الرقمية.

رسالة البرنامج:

إعداد خريجين في مجال الأمن السيبراني مزودين بالمعرفة والمهارات العملية التطبيقية المتخصصة، ولديهم الدافع للتعلم مدى الحياة والقدرة على مواكبة متطلبات العصر.

وصف البرنامج:

يعد هذا الدبلوم التدريبي التطبيقي مناسباً للمتدربين الذين يتطلعون إلى اكتساب المهارات العملية المطلوبة والمعارف المتخصصة في جميع جوانب الأمن السيبراني، حيث سيركز البرنامج على المعلومات والإجراءات الأمنية والعمليات المستخدمة في جميع أنواع بيئات الأعمال. ويهدف البرنامج الى تأهيل المتدرب للحصول على شهادات مهنية عالمية معتمدة.

يوفر هذا البرنامج للمتدربين الامكانات والقدرات التالية:

- إظهار المعرفة بمفاهيم ومصطلحات ومبادئ وطرق وأساليب أمن المعلومات والفضاء السيبراني.

- الالمام بمجموعة واسعة من التقنيات والأدوات المتاحة والطرق العملية في أمن المعلومات والفضاء السيبراني.
- التعرف على احتياجات المستخدمين في مجال تطوير نظم معلومات وبناء شبكات حاسوبية آمنة.
- إظهار المعرفة بالمبادئ الرياضية والخوارزميات الخاصة بعمليات التشفير وحماية الأنظمة والمعلومات.
- تحديد مجموعة من الحلول للطرق الحديثة والمتقدمة في اقتحام ومهاجمة البيانات والشبكات الحاسوبية.
- تقييم الثغرات ونقاط الضعف في نظم المعلومات وشبكات الحاسوب.
- تحديد وقت وتكلفة معالجة الأضرار الناتجة عن أي هجوم على نظام معلوماتي أو مؤسساتي.
- تقييم الأدوات والتقنيات المناسبة لمعالجة الأضرار الناتجة عن الاختراقات الأمنية.
- تحديد السياسات والإجراءات والخطط اللازمة لإدارة وضمان أمن المؤسسات.
- تطبيق بروتوكولات مختلفة لسرية المعلومات والشبكات.
- تطبيق مبادئ التصميم والتطوير والإدارة في إنشاء شبكات الحاسوب.
- استخدام بروتوكولات الشبكات المختلفة.
- بناء نظم المعلومات وشبكات الحاسوب الآمنة.
- إعداد وتقديم التقارير الفنية بطريقة متماسكة ومنظمة شفهية وخطية.
- استخدام أفضل الممارسات والمعايير في مجال حماية المعلومات والشبكات.
- التعامل مع شتى انواع الخروقات والحوادث على شبكات الحاسوب ونظم المعلومات.
- اكتشاف نقاط الضعف ومصادر الهجوم والاختراق من خلال مراقبة أداء شبكات الحاسوب ونظم المعلومات.
- استخدام وتطوير برمجيات التشفير وأمن المعلومات.

أهداف البرنامج:

يهدف برنامج الدبلوم التدريبي التطبيقي في الأمن السيبراني إلى:

1. تزويد الطلبة بالمعارف والكفايات النظرية والمهارات العملية التطبيقية اللازمة في مجال الأمن السيبراني.
2. إعداد كوادر بشرية مؤهلة ومتخصصة في المهن ذات العلاقة بتحليل وتصميم وتطوير وتشغيل وإدارة ومراقبة وفحص نظم وبرمجيات آمنة.
3. تمكين الطلبة من التكيف مع التطورات المستقبلية المتسارعة في مجال الأمن السيبراني من خلال تزويدهم بأسس متينة في مفاهيمه ومبادئه وأساليبه ومنهجياته الأساسية.
4. تهيئة الطلبة لخدمة مجتمعاتهم سواء كانوا أفراداً أو جماعات أو مؤسسات من خلال ضمان توفير المعلومات والبرامج والتطبيقات الآمنة لهم.
5. تمكين الطلبة من تطوير مهارات البحث، والعمل الجماعي، وحل المشكلات، والتقدم المهني، والتعلم المستقل المستمر مدى الحياة .

أهمية البرنامج:

لقد تضمنت الاستراتيجية الوطنية للأمن السيبراني للأعوام (2018-2023) في أحد محاورها وهو التعليم والتدريب، أن هناك حاجة لإعداد متخصصين مؤهلين في مجال الأمن السيبراني وتأهليهم وبناء قدراتهم وذلك لتوفير الحماية اللازمة لجميع الخدمات الالكترونية سواء الحكومية من خلال بوابة الحكومة الالكترونية او المقدمة من شركات القطاع الخاص.

وقد قامت وزارة الاتصالات وتكنولوجيا المعلومات في الأردن بدراسات تقييم احتياجات سوق العمل الأردني من القوى العاملة في قطاع تكنولوجيا المعلومات والاتصالات، حيث بينت تلك الدراسات أن الحاجة إلى مهنة متخصصين في أمن المعلومات والأمن السيبراني احتلت المرتبة الرابعة من بين أربع عشرة مهنة.

أصبحت الحواسيب الآلية والشبكات, وبالأخص الإنترنت وتطبيقاتها وخدماتها جزءاً مهماً من حياتنا اليومية حيث يتم استخدامها في مجالات عديدة ولأسباب مختلفة في البيت والعمل والمدرسة والشركات والحكومات والبنوك وغيرها. وبما أن الحواسيب والشبكات تستخدم في الاتصالات ونقل المعلومات وتبادلها عبر الإنترنت, فقد أصبح الأمن السيبراني (Cyber Security) مقوماً أساسياً في عالم تكنولوجيا المعلومات والاتصالات. فمع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لآخر، فقد أصبح أمن تلك البيانات والمعلومات يشكل هاجسًا وموضوعًا حيويًا مهمًا للغاية. حيث يعتبر أمن المعلومات علم مختص بتأمين المعلومات المتداولة عبر شبكة الإنترنت من المخاطر التي تهددها. كما يعتبر مجال أمن المعلومات من أكثر المجالات حيوية في قطاع تكنولوجيا المعلومات لارتباطه بأكثر من تخصص بشكل فعال ومؤثر.

وقد تضمن قانون المعاملات الالكترونية الأردني رقم (15) لسنة 2015 في مواده ما يؤكد أهمية حماية أمن وسرية وخصوصية المعاملات الالكترونية ونقل وتبادل البيانات والمعلومات، وبناءً على ذلك القانون قام البنك المركزي الأردني بإصدار تعليمات سميت بـ "تعليمات التكيف مع المخاطر السيبرانية" وذلك لإدارة أمن ومخاطر تكنولوجيا المعلومات في البنوك والمؤسسات المالية.

ويعمل الأردن على تمكين الإدارة الفاعلة للبيئة الوطنية السيبرانية، حيث ظهر ذلك من خلال إصدار الأردن للاستراتيجية الوطنية للأمن السيبراني، بالإضافة إلى إطلاق مجموعة من السياسات الوطنية للأمن السيبراني التي تعمل على تحسين الإدارة العامة والإدارة الفنية لدى الجهات الحكومية، وإعداد مسودة قانون للأمن السيبراني والتي تهدف إلى إنشاء مركز يُعنى بإدارة الامن السيبراني على المستوى الوطني.

وقد حرص الأردن على تحسين بيئته السيبرانية حيث تقدم الأردن 18 مرتبة عالمياً، ومرتبتين على المستوى العربي في بيئة الأمن السيبراني وفق ما أظهر التقرير الصادر عن الاتحاد الدولي للاتصالات التابع للأمم المتحدة، والخاص بالإصدار الثالث من التقرير العالمي للأمن السيبراني (Global Cybersecurity Index 2018). حيث يستند التقييم على خمسة محاور من ضمنها بناء القدرات الذي يشير إلى الحاجة إلى وجود الكفاءات المؤهلة والمتخصصة في الأمن السيبراني.

وبناءً على ما تقدم قامت كلية تكنولوجيا المعلومات بدراسة العديد من الأبحاث والدراسات والإحصاءات والتقارير حيث أظهرت نتائجها وتوصياتها ومؤشراتها أن مجال الأمن السيبراني مطلوب محلياً وإقليمياً وعالمياً، ومن هنا برزت فكرة استحداث برنامج دبلوم تدريبي تطبيقي يختص بالأمن السيبراني.

مجالات العمل وحاجات السوق:

قامت كلية تكنولوجيا المعلومات بدراسة حاجة السوق المحلي وكذلك السوق الإقليمي وذلك بالبحث عن فرص العمل المتاحة من خلال مواقع التوظيف حيث أكدت الأرقام أن السوق المحلي والإقليمي بحاجة الى موظفين لديهم القدرة على تحليل وتصميم وتطوير وتشغيل وإدارة ومراقبة وفحص نظم وبرمجيات آمنة في المؤسسات والشركات العامة والخاصة.

يزيد برنامج الدبلوم التدريبي التطبيقي في الأمن السيبراني من الفرص المتاحة للعمل أمام المنتسبين إليه في أسواق العمل المحلية والإقليمية والدولية، لما يوفره من المهارات والخبرات العملية اللازمة لسوق العمل، وذلك من خلال طرح العديد من المواضيع المتنوعة في أمن المعلومات والفضاء السيبراني.
يتيح برنامج الدبلوم للراغبين بالالتحاق به اكتساب المهارات اللازمة لتصميم البيئة الآمنة واستخدام الأدوات التي تساعد على الحماية والتدقيق والتحقيق واكتشاف الجرائم الإلكترونية وكيفية وضع الحلول المناسبة للحماية. كما سيزود البرنامج الطلبة بالمهارات اللازمة لتطبيق المبادئ والمفاهيم المتقدمة والمتعلقة بتطوير وإدارة نظم معلومات آمنة في المؤسسات الحكومية ومؤسسات القطاع الخاص.

هنالك عدد كبير من الوظائف يستطيع خريج هذا الدبلوم التدريبي المنافسة عليها منها:

- مسؤول أمن تقنية المعلومات
- فني أمن الشبكات والمعلومات
- فني أمن الشبكات اللاسلكية
- فني تحليل الجرائم الإلكترونية
- فني تحليل نظم أمنية وتوكيد جودة المعلومات
- فني تدقيق أمن برمجيات
- فني أمن المعلومات
- فني اختبار الاختراق
- فني التحليل الجنائي
- فني الأمن الإلكتروني
- فني متخصص في الحوادث والتهديدات الالكترونية
- فني تطور برامج آمنه
- عضو مشروع تقنية المعلومات
- فني الجرائم الإلكترونية
- فني في الأدلة الجنائية الحاسوبية.

الخطة الدراسية:

يتضمن الجدول (1) الخطة الدراسية المقترحة لبرنامج الدبلوم التدريبي التطبيقي في الأمن السيبراني باللغتين العربية والإنجليزية، حيث تم إعداد هذه الخطة من قبل لجنة من أعضاء الهيئة التدريسية في كلية تكنولوجيا المعلومات من ذوي العلاقة بمجال أمن المعلومات وبالشراكة مع متخصصين من شركات متخصصة في مجال الأمن السيبراني، كما يتضمن المرفق رقم 1 المحتوى العلمي للمواد الدراسية.

الفئة المستهدفة:

طلبة الثانوية العامة أو الذين لم يحالفهم الحظ في امتحان الثانوية العامة، وكذلك المهتمين من خريجي التخصصات الهندسية وتكنولوجيا المعلومات.

مدة الدراسة وعدد الساعات التدريسية:

عدد ساعات الخطة الدراسية لبرنامج الدبلوم التدريبي هي (30) ساعة معتمدة (كما في الجدول رقم 1) بواقع (10) مواد دراسية موزعة على فصلين دراسيين، مدة الفصل الدراسي (4) اشهر ونصف.

عدد الساعات النظري والعملي في الفصل الدراسي الواحد هي (225) ساعة تدريس (45 ساعة دراسية لكل مادة في الخطة)، لذا يكون المجموع الكلي للساعات النظري والعملي خلال الفصلين الدراسيين (450) ساعة تغطى خلال (9) اشهر.

منهجية الدراسة:
نظراً لظروف جائحة كورونا، فإن الدراسة ستكون عن بعد ومن خلال المنصة التعليمية المعتمدة في الجامعة (Microsoft Teams).

لغة الدراسة:
سيتم اعتماد اللغتين العربية و الانجليزية في تدريس مواد برنامج الدبلوم التدريبي.

الشهادات:
تصدر الشهادات من جامعة فيلادلفيا-كلية تكنولوجيا المعلومات، ويتم تصديقها من وزارة التعليم العالي والبحث العلمي الأردنية.

الجدول (1): الخطة الدراسية المقترحة لبرنامج الدبلوم التدريبي في الامن السيبراني.

Module No.	Module Name	Credit Hours
CS701	**أمن نظم المعلومات**(Information System Security)	3
CS703	**البرمجة بلغة بايثون** (Programming with Python)	3
CS707	**شبكات وأمن نظم لينكس** (Linux Networking and Security)	3
CS704	**القرصنة والاختبار الأخلاقي** (Ethical Hacking and Testing)	3
CS726	**تحليل بيانات الأمن السيبراني** (Cybersecurity Data Analysis)	3
CS705	**الأمن التشغيلي للبنية التحتية الحرجة** (Operational Security for Critical Infrastructure)	3
CS708	**تقنيات القرصنة المتقدمة** (Advanced Hacking Techniques)	3
CS710	**إجراء اختبارات الاختراق والأمن (** Conducting Penetration and Security Tests)	3
CS706	**التشفير** (Cryptography)	3
CS727	**مشروع الأمن السيبراني** (Cybersecurity Project)	3

مرفق رقم (1)

وصف المواد الواردة في الخطة الدراسية:

Module Name
أمن نظم المعلومات Information System Security Description: In this course students will learn the fundamentals of information security including design and implementation of secure systems, security assessment, and computer security ethics. Students will utilize a variety of cutting edge technologies and labs in many hands-on learning activities.
البرمجة بلغة بايثون Programming with Python Description: Having mastered the core concepts of Python from our beginners Python course, students will learn more advanced Python programming with a focus on enterprise development. Students will use Python to interact with databases and GUI's and perform Network Programming. This is a practical hands on course, designed to teach students practical programming for the real business application.
شبكات وأمن نظم لينكس Networking and Security Linux Description: This course focuses on configuring a secure Linux network using command line and graphical utilities. Emphasis is placed on file sharing technologies such as the Network File System, NetWare's NCP file sharing, and File Transfer Protocol. Additional topics include making data secure, user security, file security, and network intrusion detection. Students will be required to take on the role of problem solvers and apply the concepts presented to situations that might occur in a work environment.
القرصنة والاختبار الأخلاقي Ethical Hacking and Testing Description: The Ethical Hacking and Testing course focus on how perimeter defenses work, how intruders escalate privileges, and methods of securing systems. Additional topics include intrusion detection, policy creation, social engineering, DoS attacks, buffer overflows, and virus creation.
تحليل بيانات الأمن السيبراني Cybersecurity Data Analysis Description: This course teaches students how to identify typical sources of institutional knowledge, including Customer Relationship Management (CRM) applications, inventory management systems, transaction data, social media, marketing sources, industry systems. Students will compare and contrast structured and unstructured data in order to summarize how data can drive business decisions. The course also covers specific tactics for working with cloud-based data, including cloud-native data, migrating data to or from the cloud, backup procedures, security issues, and user training. Students will learn ways to determine relationships between organizational efforts and business outcomes, extrapolate information using data obtained from new and traditional data sources, and ways to analyze and represent data. Students will also learn how ethics and security are vital parts of a Data Analyst's responsibilities. The Data Analyst can compile the data from many sources, prepare and deliver an objective and unbiased presentation.
الأمن التشغيلي للبنية التحتية الحرجة Security for Critical Infrastructure Operational Description: Critical Infrastructure is that whose continuous operation is deemed necessary to ensure the security of a given nation, its economy, and

the public's health and/or safety, like (ESADA and SS7). The Operational Security for Critical Infrastructure course is designed to provide students with the knowledge to manage and operate critical infrastructure surrounding the protection of systems, networks, and assets.
تقنيات القرصنة المتقدمة Hacking Techniques Advanced Description: The Advanced Hacking Techniques course focuses on how perimeter defenses work, how intruders escalate privileges, and methods of securing systems. Additional topics include intrusion detection, policy creation, social engineering, DoS attacks, buffer overflows, and virus creation.
إجراء اختبارات الاختراق والأمن Security Tests Conducting Penetration and Description: The Conducting Penetration and Security Test course focuses on mastery of the international standard for penetration testing. Topics include customers and legal agreements ,penetration testing planning and scheduling, information gathering, external and internal network penetration testing, router penetration testing ,firewalls penetration testing, intrusion detection system penetration testing, wireless networks penetration testing; password cracking penetration testing, social engineering penetration testing, PDA and cell phone penetration testing, and penetration testing report and documentation writing.
التشفير Cryptography Description: The course covers the basics concepts of cryptography including :**traditional ciphers, block ciphers, stream ciphers, public and private key cryptosystems** .The course also includes the theory of hash functions, authentication systems, network security protocols and malicious logic.

مرفق رقم (2)
شهادات التأهيل المهني

معلومات عن شهادات عالمية معتمدة يمكن للمتدرب الحصول عليها أثناء مدة البرنامج أو بعد إنجازه:

1. Certified Ethical Hacker (CEH)

Certified Ethical Hacker CEH will teach you the latest commercial-grade hacking tools, techniques, and methodologies used by hackers and information security professionals to lawfully hack an organization.

2. Security+

Security+ is a global certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career.

3. Offensive Security Certified Professional – Penetration Testing (OSCP)

This online ethical hacking course is self-paced. It introduces penetration testing tools and techniques via hands-on experience. PWK trains not only the skills, but also the mindset required to be a successful penetration tester.

4. Certified SOC Analyst (CSA)

CSA is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry.