

جامعة العلوم والتكنولوجيا الأردنية

كلية تكنولوجيا الحاسوب والمعلومات
قسم الأمن السيبراني

الخطة الدراسية

للحصول على درجة البكالوريوس
في

الأمن السيبراني

عمادة شؤون الطلبة:
تلفون: 7201000 – 2 – (962) فرعي (22543)
فاكس: 7201043 – 2 – (962)
بريد الكتروني: studentaffairs@just.edu.jo

وحدة القبول والتسجيل:
تلفون: 7201000 – 2 – (962) فرعي (27163)
فاكس: 7201027 – 2 – (962)
بريد الكتروني: register@just.edu.jo

مكتب الطلبة العرب والأجانب:

تلفون: 7201000 – 2 – (962) فرعي – (23040) أو (23048)
فاكس: 7201025 – 2 – (962)
بريد الكتروني: iso@just.edu.jo

جامعة العلوم والتكنولوجيا الأردنية:
ص.ب 3030 اربد – 22110 – الأردن
تلفون: 7201000 – 2 – (962)
فاكس: 7095141 – 2 – (962)
بريد الكتروني: prsd@just.edu.jo

كلية الحاسوب وتكنولوجيا المعلومات:
تلفون: 7201000 – 2 – (962) فرعي (20000)
فاكس: 7201077 – 2 – (962)
بريد الكتروني: cit@just.edu.jo

قسم الأمن السيبراني:
تلفون: 7201000 – 2 – (962) فرعي (23903)
فاكس: 7201077 – 2 – (962)
بريد الكتروني: aiiad@just.edu.jo

الرؤية:

نحو برنامج فريد ومتميزو تقني في الأمن السيبراني لتغطية النقص الملح في سوق العمل المحلي والعالمي بمختصين بأعلى درجات الكفاءة والمهنية

الرسالة:

رسالتنا تكمن بتخريج مختصين في مجال الأمن السيبراني والمحافظة على موائمة قدراتهم لأحدث المعايير في حقل تكنولوجيا المعلومات دائم التطور. كذلك، تخريج مختصين في مجال الامن السيبراني قادرين على توظيف أحدث الطرق الأكاديمية والصناعية من اجل بناء أنظمة برمجيات عالية الكفاءة

ويتم ذلك من خلال كادر قادر على تعزيز التفاهم المتبادل بين الكادر التعليمي والطلاب من أجل خلق بيئة ممتعة للتعلم والتعليم، وإعداد بحوث نظرية وتطبيقية عالية الجودة، وتعزيز التعاون المستمر والتواصل مع الصناعة المحلية والاقليمية من أجل الحفاظ على برامج تعليمية قادرة على خدمة الصناعة ورفدها بالمختصين المناسبين لحاجتها

الأهداف:

- تطوير وتقديم وتنفيذ خطة دراسية متشعبة في مجال الأمن السيبراني لدعم الجيل القادم من محترفي الأمن السيبراني أكاديميا وعمليا.
- تطوير البنية التحتية اللازمة لدعم البحث والتعليم في مجالات التحليلات الأمنية والقرصنة الأخلاقية وأمن الشبكة والبرمجة الآمنة.
- بناء الكفاءات في مجال الأمن السيبراني للنهوض بمجال الاختراق الأخلاقي واختبار الاختراق من خلال تطوير طرق جديدة لاكتشاف نقاط الضعف والقضايا في أنظمة وشبكات الحاسوب.
- بدء شراكات حكومية، وصناعية للبحث، والتعليم، والتدريب.

المخرجات:

سيكون لخريجي برنامج الأمن السيبراني القدرة على:

1. تحليل مشكلة حاسوبية معقدة وتطبيق مبادئ الحوسبة وغيرها من التخصصات ذات الصلة لتحديد الحلول.

2. تصميم وتنفيذ وتقييم الحلول المبنية على الحوسبة لتلبية مجموعة معينة من متطلبات الحوسبة في سياق انضباط البرنامج.

3. التواصل الفعال في مجموعة متنوعة من مجالات العمل المختلفة.

4. الاعتراف بالمسؤوليات المهنية وإصدار أحكام مبنية على المعرفة في ممارسة الحوسبة استناداً إلى المبادئ القانونية والأخلاقية.

5. العمل بفاعلية كعضو أو قائد فريق مشارك في أنشطة مناسبة لضوابط البرنامج.

6. تطبيق المبادئ والممارسات الأمنية للحفاظ على سير العمليات في ظل وجود المخاطر والتحديات.

مدلول رموز وأرقام مسابقات الأمن السيبراني

المنزلة	المعنى	التوضيح	
المئات	مستوى المساق	1	السنة الأولى
		2	السنة الثانية
		3	السنة الثالثة
		4	السنة الرابعة
العشرات	تخصص وموضوع المساق	0	مبادئ أساسية
		1	البرمجة
		2	قواعد البيانات
		3	-
		4	الشبكات
		5	التطبيقات
		6	إخفاء المعلومات
		7	الأنظمة والبرامج
		8	متفرقات
9	مواضيع خاصة وتدريب		
الاحاد	ترتيب المساق	الرقم التسلسلي للمساق ضمن تخصص وموضوع المساق	

جامعة العلوم والتكنولوجيا الأردنية
الخطة الدراسية للحصول على درجة البكالوريوس في الأمن السيبراني

تمنح درجة البكالوريوس في الأمن السيبراني في كلية تكنولوجيا الحاسوب والمعلومات بجامعة العلوم والتكنولوجيا الأردنية بعد إنهاء (132 س.م) موزعة حسب ما هو مبين في جدول (1).

جدول (1): توزيع الساعات لتخصص الأمن السيبراني

المجموع	الساعات الاختيارية	الساعات الإلزامية	المتطلبات
25	9	16	متطلبات الجامعة
24	0	24	متطلبات الكلية
83	12	71	متطلبات القسم
132	21	111	المجموع

وبعد تحقيق الشروط المنصوص عليها في تعليمات منح درجة البكالوريوس الصادرة عن مجلس العمداء بموجب نظام منح الدرجات العلمية والشهادات في جامعة العلوم والتكنولوجيا الأردنية.

أولاً: متطلبات الجامعة

ويخصص لها (25 س.م) معتمدة تنفرد إلى متطلبات إجبارية بواقع (16 س.م) ومتطلبات اختيارية بواقع (9 س.م) حسب ما نصت عليه تعليمات منح درجة البكالوريوس.

ثانياً: متطلبات الكلية

ويخصص لها (24 س.م) إجبارية كما هو مبين في جدول رقم (2).

جدول (2): متطلبات الكلية الإلزامية

رمز المساق ورقمه	اسم المساق	الساعات المعتمدة	الساعات الأسبوعية		المتطلب السابق	طريقة التدريس
			نظري	عملي		
ر 101	تفاضل وتكامل (1)	3	3	0	-	وجاهي
ر 102	تفاضل وتكامل (2)	3	3	0	النجاح ر 101	وجاهي
ر 241	الرياضيات المنقطعة	3	3	0	-	وجاهي
ع ح 101	مقدمة في البرمجة	3	2	0	ن م 99 أو متزامن	وجاهي
هـ ب 103	مقدمة الى تكنولوجيا المعلومات	3	3	0	متزامن ع ح 101	عن بعد (متزامن الحضور)
هـ ب 112	مقدمة في البرمجة الكينونية	3	2	0	النجاح في ع ح 101	مدمج (1+1)
ع ح 211	تراكيب البيانات	3	3	0	ر 241 + النجاح في هـ ب 112	مدمج (1+1)
ن م 221	أساسيات قواعد البيانات	3	3	0	ع ح 211	وجاهي

ثالثاً: متطلبات القسم

ويخصص لها (83 س.م) موزعة على النحو التالي:

- أ. متطلبات إجبارية (71 س.م) كما هو مبين في جدول (3).
 ب. متطلبات إختيارية بواقع (12 س.م) يختارها الطالب من قائمة المساقات المبينة في جدول (4) شريطة أن يكون 9 س.م منها على الأقل من قسم الأمن السيبراني*.

جدول (3): متطلبات القسم الاجبارية

رمز المساق ورقمه	اسم المساق	الساعات المعتمدة	الساعات الاسبوعية		المتطلب السابق	طريقة التدريس
			نظري	عملي		
أس 101	أساسيات الأمن السيبراني	3	3	0	ع ح 101	وجاهي
أس 111	مختبر لغة Assembly	1	0	3	هـ ب 112 أو متزامن	وجاهي
أس 201	أخلاقيات الامن السيبراني	1	1	0	أس 101	عن بعد (متزامن الحضور)
أس 211	لغة برمجة مرئية مختارة	2	0	6	هـ ب 112	مدمج (1+1)
أس 261	نظرية التشفير	3	3	0	هـ ب 112، ر 233	وجاهي
أس 341	شبكات الحاسوب	3	3	0	ع ح 284	وجاهي
أس 342	مختبر شبكات الحاسوب	1	0	3	أس 341 أو متزامن	عن بعد (متزامن الحضور)
أس 343	أمن شبكات الحاسوب	2	2	0	أس 341، أس 261، أس 371	وجاهي
أس 344	مختبر أمن شبكات الحاسوب	1	0	3	أس 343 أو متزامن	عن بعد (متزامن الحضور)
أس 345	حماية شبكات الحاسوب	2	2	0	أس 344	وجاهي
أس 346	مختبر حماية شبكات الحاسوب	1	0	3	أس 345 أو متزامن	عن بعد (متزامن الحضور)
أس 371	مختبر نظام التشغيل Linux	1	0	3	ع ح 375	عن بعد (متزامن الحضور)
أس 381	ادارة المخاطر	3	3	0	أس 101	مدمج (1+1)
أس 391	التدريب الميداني	3	0	0	انهاء 90 ساعة بنجاح	وجاهي
أس 411	هندسة البرمجيات العكسية	2	0	6	أس 101، أس 111، أس 211	وجاهي
اس 431	أمن البرمجيات	3	0	0	أس 344، أس 211، أس 452 أو متزامن	مدمج (1+1)
أس 451	أمن البيانات التحليلي	3	2	3	أس 343، أس 371، أس 111	وجاهي
أس 452	أمن الويب	3	2	3	ن م 201، أس 343 أو متزامن، ن م 221	وجاهي
أس 481	الاختراق الأخلاقي (1)	3	1	6	أس 344	وجاهي
أس 482	الاختراق الأخلاقي (2)	3	0	9	أس 481، أس 452	وجاهي
أس 483	التحقيق الجنائي الرقمي	2	2	0	أس 411، أس 451	مدمج (1+1)
أس 484	مختبر التحقيق الجنائي الرقمي	1	0	3	أس 483 أو متزامن	عن بعد (متزامن الحضور)
أس 491	مشروع التخرج (1)	1	1	0	انهاء 90 ساعة بنجاح	وجاهي
أس 492	مشروع التخرج (2)	2	2	0	اس 491	وجاهي
ع ح 284	تحليل وتصميم الخوارزميات	3	3	0	ع ح 211	وجاهي
ع ح 362	الذكاء الاصطناعي	3	3	0	ع ح 284	وجاهي
ع ح 375	مبادئ نظم التشغيل الحديثة	3	3	0	ع ح 211	وجاهي
ن م 201	مقدمة في تصميم صفحات الوب	1	0	3	هـ ب 112	وجاهي
ن م 203	مهارات الاتصال واخلاقيات المهنة	2	2	0	-	مدمج
ن م 332	تحليل وتصميم النظم	3	3	0	ن م 221	وجاهي
ر 140	مبادئ الجبر الخطي	3	3	0	-	وجاهي

*يعنى الطالب من دراسة 3 ساعات معتمدة من المساقات الاختيارية (جدول 4) إذا التحق بأحد الأكاديميات العالمية المتخصصة في طرح دورات تقنية او التحق بدورة تدريبية تقنية تطرح في الكلية يزيد فيه عدد الساعات التدريبية عن 150 ساعة شرط حصوله على الشهادة المعتمدة عالمياً لتلك الدورة.

ر 233	احصاء واحتمالات لطلبة الحاسوب	3	3	0	ر 102	وجاهي
-------	-------------------------------	---	---	---	-------	-------

جدول (4): متطلبات القسم الاختيارية

رمز ورقم المساق	اسم المساق	الساعات المعتمدة	الساعات الاسبوعية		المتطلب السابق	طريقة التدريس
			نظري	عملي		
أ س 321	أمن قواعد البيانات	3	2	3	أ س 261، ن م 221	مدمج (1+1)
أ س 412	برمجة تطبيقات المحمول	3	0	3	هدب 112	وجاهي
أ س 453	أمن الحوسبة السحابية	3	3	0	أ س 452	مدمج (1+1)
أ س 454	أمن انترنت الأشياء	3	3	0	أ س 343	مدمج (1+1)
أ س 455	أمن وخصوصية نظم المعلومات الصحية	3	3	0	أ س 101	مدمج (1+1)
أ س 456	التعلم العميق	3	3	0	ع ح 362	وجاهي
أ س 461	مقدمة الى علم اخفاء المعلومات	3	2	3	أ س 261	مدمج (1+1)
أ س 462	نظرية التشفير المتقدمة	3	3	0	أ س 261	وجاهي
أ س 471	أمن نظم التشغيل	3	2	3	أ س 261، أ س 371	وجاهي
أ س 485	طرق منهجية في الأمن السيبراني	3	3	0	أ س 261	وجاهي
أ س 493-أ	موضوعات خاصة في الأمن السيبراني (1)	3	3	0	موافقة القسم	عن بعد (متزامن الحضور)
أ س 493-ب	موضوعات خاصة في الأمن السيبراني (2)	3	3	0	موافقة القسم	عن بعد (متزامن الحضور)
-	مساق من أقسام الكلية الأخرى (مستوى 400 فما فوق)	3	3	0	موافقة القسم	وجاهي

**الخطة الاسترشادية
للحصول على درجة البكالوريوس في الأمن السيبراني**

السنة الأولى

الفصل الأول			
رقم ورمز المساق	اسم المساق	الساعات المعتمدة	المتطلب السابق
ر 101	تفاضل وتكامل (1)	3	-
ر 241	رياضيات متقطعة	3	-
ع ح 101	مقدمة في البرمجة	3	ن م 99 أو متزامن
ع ح 101	مقدمة في البرمجة (عملي)	0	ع ح 101 أو متزامن
ل غ 101	اللغة الإنجليزية ومهارات الاتصال والتواصل	3	النجاح في ل غ 99 أو اجتياز امتحان المستوى بعلامة لا تقل عن 50%.
ع أ 110	القيادة المسؤولة المجتمعية	3	-
هد ب 103	مقدمة الى تكنولوجيا المعلومات	3	متزامن مع ع ح 101
مجموع الساعات:		18	

الفصل الثاني			
رقم ورمز المساق	اسم المساق	الساعات المعتمدة	المتطلب السابق
ر 102	تفاضل وتكامل (2)	3	ر 101
ر 140	مبادئ الجبر الخطي	3	-
هد ب 112	مقدمة في البرمجة الكينونية	3	النجاح في ع ح 101
هد ب 112	مقدمة في البرمجة الكينونية (عملي)	0	متزامن مع هد ب 112
ل غ 103	المهارات الحياتية	2	-
أ س 101	أساسيات الأمن السيبراني	3	ع ح 101
أ س 111	لغة برمجة Assembly	1	هد ب 112 أو متزامن
مجموع الساعات:		15	

السنة الثانية

الفصل الأول			
رقم ورمز المساق	اسم المساق	الساعات المعتمدة	المتطلب السابق
ع 102	اللغة العربية ومهارات الاتصال والتواصل	3	-
ع ح 211	تراكيب البيانات	3	النجاح في ع ح 112 + ر 241
أ س 211	لغة برمجة مرئية مختارة	2	ع ح 112
ر 233	احصاء واحتمالات لطلبة الحاسوب	3	ر 102
ن م 201	مقدمة في تصميم صفحات الويب	1	هد ب 112
ن م 203	مهارات الاتصال واخلاقيات المهنة	2	-
-	متطلب جامعة اختياري	3	-
مجموع الساعات:		17	

الفصل الثاني			
رقم ورمز المساق	اسم المساق	الساعات المعتمدة	المتطلب السابق
أ س 201	اخلاقيات الأمن السيبراني	1	أ س 101
ع ح 284	تحليل وتصميم الخوارزميات	3	ع ح 211
ن م 221	أساسيات قواعد البيانات	3	ع ح 211
ع ح 375	مبادئ نظم التشغيل الحديثة	3	ع ح 211
ع أ 119	الريادة و الابداع	2	-
أ س 261	نظرية التشفير	3	ع ح 112 + ر 233
-	متطلب جامعة اختياري	3	-
مجموع الساعات:		18	

السنة الثالثة

الفصل الأول			
رقم ورمز المساق	اسم المساق	الساعات المعتمدة	المتطلب السابق
ع 100	علوم عسكرية	3	-
ن م 332	تحليل وتصميم النظم	3	ن م 221
أ س 341	شبكات الحاسوب	3	ع ح 284
أ س 342	مختبر شبكات الحاسوب	1	أ س 341 أو متزامن
أ س 371	مختبر نظام التشغيل Linux	1	ع ح 375
ع ح 362	الذكاء الاصطناعي	3	ع ح 284
-	متطلب قسم اختياري	3	-
مجموع الساعات:		17	

الفصل الثاني			
رقم ورمز المساق	اسم المساق	الساعات المعتمدة	المتطلب السابق
أ س 343	أمن شبكات الحاسوب	2	أ س 341+أ س 261+أ س 371
أ س 381	ادارة المخاطر	3	أ س 101
أ س 411	هندسة البرمجيات العكسية	2	أ س 111+أ س 101+أ س 211
أ س 344	مختبر أمن شبكات الحاسوب	1	أ س 343 أو متزامن
أ س 452	أمن الويب	3	ن م 201+أ س 343 أو متزامن + ن م 221
-	متطلب جامعة اختياري	3	-
-	متطلب قسم اختياري	3	-
مجموع الساعات:		17	

الفصل الصيفي			
رقم ورمز المساق	اسم المساق	الساعات المعتمدة	المتطلب السابق
س 391	التدريب الميداني	3	بعد إنهاء 90 س.م
مجموع الساعات:		3	

السنة الرابعة

الفصل الأول			
رقم ورمز المساق	اسم المساق	الساعات المعتمدة	المتطلب السابق
أ س 345	حماية شبكات الحاسوب	2	أ س 344
أ س 431	أمن البرمجيات	3	أ س 344+أ س 211+أ س 452 (أو متزامن)
أ س 346	مختبر حماية الشبكات	1	أ س 345 (أو متزامن)
أ س 451	أمن البيانات التحليلي	3	أ س 343+أ س 371 +أ س 111
أ س 481	الاختراق الأخلاقي (1)	3	أ س 344
-	متطلب قسم اختياري	3	-
أ س 491	مشروع التخرج (1)	1	انهاء 90 ساعة بنجاح
مجموع الساعات:		16	

الفصل الثاني			
رقم ورمز المساق	اسم المساق	الساعات المعتمدة	المتطلب السابق
أ س 482	الاختراق الأخلاقي (2)	3	أ س 481 + أ س 452
أ س 483	التحقيق الجنائي الرقمي	2	أ س 411+أ س 451
أ س 484	مختبر التحقيق الجنائي الرقمي	1	أ س 483 (أو متزامن)
أ س 492	مشروع التخرج (2)	2	أ س 491
-	متطلب قسم اختياري	3	-
مجموع الساعات:		11	

وصف المساقات

أ س 101 أساسيات الأمن السيبراني

المتطلب السابق: ع ح 101

3 س.م = (3نظري، 0 عملي)

يغطي هذا المساق مقدمة حول موضوعات الأمان الكلاسيكية، مثل التشفير المطبق، والمصادقة، وضوابط الوصول للمعلومات، ومنع التطفل واكتشافه، وأمان قاعدة البيانات، وأمن الويب، وأمن الأنظمة والبرامج الضارة. علاوة على ذلك، فإنه يغطي الموضوعات المتعلقة بالأخلاقيات والقوانين في مجال الأمن السيبراني.

أ س 111 لغة برمجة Assembly

المتطلب السابق: ع ح 112 أو مترامن

1 س.م = (0نظري، 3 عملي)

يركز هذا المساق على تنظيم وتشغيل أنظمة الحاسوب على مستوى لغة التجميع. يغطي المساق تعيين العبارات والتراكيبات بلغة عالية المستوى إلى المقابل لها من تعليمات الآلة، بالإضافة إلى التمثيل الداخلي لأنواع البيانات وهيكلتها. يتم من خلال هذا المساق ممارسة البرمجة مع لغة تجميع لتوفير التطبيق العملي للمفاهيم المقدمة.

أ س 201 أخلاقيات الامن السيبراني

المتطلب السابق: أ س 101

1 س.م = (1نظري، 0 عملي)

يقدم هذا المساق القضايا الاخلاقية في الامن السيبراني. ويتضمن المساق: تعريف الاخلاق، المواقف الاخلاقية المختلفة، المسؤولية الاحترافية، الممارسات المعرفية العادلة، النظم الاخلاقية، القضايا الاخلاقية في نشر العيوب الامنية، وعلاقة الاخلاقيات بالقانون. كما يتضمن المساق تقديم وتحليل هياكل العمل الاخلاقية السائدة والنظريات المعيارية.

أ س 211 لغة برمجة مرئية مختارة

المتطلب السابق: ع ح 112

2 س.م = (0نظري، 6 عملي)

يغطي هذا المساق اساسيات واجهات الاستخدام الرسومية، البرمجة الموجهة بالاحداث، الكائنات والخصائص، القوائم، الاجراءات، هياكل السيطرة، ومعالجة ملفات قواعد البيانات. كما يشرح هذا المساق كيفية استخدام وتطوير مكونات واجهات الاستخدام الرسومية كالأزرار و صناديق النصوص في بيئات التطوير المتكاملة.

أ س 261 نظرية التشفير

المتطلب السابق: ع ح 112 + ر 233

3 س.م = (3نظري، 0 عملي)

يغطي هذا المساق المفاهيم الاساسية في علم التشفير مثل التشفير وفك التشفير، التحقق من المرسل، موثوقية البيانات، عدم التنصل، تصنيف الهجمات (النص المشفر فقط، النص الأصلي المعروف، النص الأصلي المحدد، النص المشفر المحدد)، التشفير المتماثل (خوارزميات DES و AES)، التشفير غير المتماثل (خوارزمية RSA)، الأمن المبني على نظرية المعلومات (سر المرة الواحدة، نظرية شانون)، تبادل المفاتيح والتوقيعات الرقمية.

أ س 321 أمن قواعد البيانات

المتطلب السابق: أ س 261 + ن م 221

3 س.م = (2نظري، 3 عملي)

يوفر هذا المساق نظرة عامة عن مبادئ وتقنيات امن قواعد البيانات. حيث يغطي نماذج أمن قواعد البيانات، والتحكم في الوصول وتطبيقه على أمن قاعدة البيانات، النموذج العلائقي الأمن متعدد المستويات، المصادقة، إدارة الثقة، حماية الخصوصية، وتدقيق البيانات. يتضمن المساق تحديد المخاطر والتهديدات ونقاط الضعف في أنظمة قواعد البيانات. علاوة على ذلك يوفر المساق مجموعة من التجارب العملية التي توفر خبرة عملية في هذا الموضوع.

أ س 341 شبكات الحاسوب

المتطلب السابق: ع ح 284

3 س.م = (3نظري، 0 عملي)

يغطي هذا المساق موضوعات حول معماريات الشبكة وبروتوكولات طبقة التطبيقات مثل HTTP و FTP وبروتوكولات طبقة الإرسال مثل TCP و UDP وخدمات طبقة الشبكة مثل بروتوكولات التوجيه و IPv4 و IPv6 وخدمات طبقة ارتباط البيانات مثل اكتشاف الأخطاء وتصحيحها، التحكم في الاستخدام المتعدد ومبادئ الشبكات اللاسلكية.

أ س 342 مختبر شبكات الحاسوب

المتطلب السابق: أ س 341 (أو مترامن)

1 س.م = (0نظري، 3 عملي)

يتكون هذا المختبر من تجارب لتصميم وتطبيق وتحليل وتقويم بروتوكولات شبكات الحاسوب. كما ويحتوي على تجارب لتقويم بروتوكولات التوجيه الثابت والديناميكي مثل: RIP و OSPF و BGP. وتقويم وتحليل بروتوكولات TCP و UDP، والتركيز على إعدادات DHCP و NAT، وتحليل البيانات المحمولة عبر الشبكة باستخدام أدوات التنصت.

أ س 343 أمن شبكات الحاسوب

المتطلب السابق: أ س 341 + أ س 261 + أ س 371

2 س.م = (2نظري، 0 عملي)

يغطي هذا المساق مبادئ وتقنيات أمن الشبكات والاتصالات. حيث يوضح العديد من هجمات الشبكات مثل DoS و DDoS واغراق الـ MAC وانتحال الـ DHCP. بالإضافة الى أنواع مختلفة من الإجراءات المضادة مثل جدران الحماية وأنظمة اكتشاف التدخل التي يتم استخدامها لمنع واكتشاف الهجمات. يناقش المساق آليات عمل بروتوكولات الأمان مثل SSL / TLS و IPsec و SSH.

أ س 344 مختبر أمن شبكات الحاسوب

المتطلب السابق: أ س 343 (أو مترامن)

1 س.م = (0نظري، 3 عملي)

يغطي هذا المساق مجموعة من التجارب العملية لدراسة بروتوكولات الأمان مثل SSL/TLS و SSH و IPsec. علاوة على ذلك، يحتوي على تجارب حول تنفيذ هجمات ضد بروتوكولات الشبكة مثل TCP و UDP و ARP وهجمات التعرف على حركة المرور واختراق DNS واغراق SYN ومسح المنافذ والتحكم في الوصول وأنظمة كشف التسلل وجدران الحماية.

أ س 345 حماية شبكات الحاسوب

المتطلب السابق: أ س 344

2 س.م = (2نظري، 0 عملي)

يقدم هذا المساق دراسة أساسية عن طرق الدفاع عن الشبكة، وقضايا الأمان والضعف ذات الصلة لشبكات الحاسوب، والأدوات الشائعة المتاحة لتحليل حزم الشبكة واستغلالها. تشمل الموضوعات التي سيتم تناولها مراجعة المفاهيم والمبادئ الأساسية المتعلقة بالدفاع عن الشبكة (بروتوكولات الشبكات والتشفير، وضمان اكتمال المهمة، وتطوير سياسة الشبكة وإنفاذها، وما إلى ذلك)، وتطوير الشبكة الأمانة (التحكم في الوصول إلى الشبكة، وتكوين الشبكة بشكل آمن، وتنفيذ جدران الحماية، والشبكات الافتراضية الآمنة، إلخ)، وتقنيات الدفاع المتقدمة عن الشبكة (البرامج التي يتم من خلالها اصطياد مخترقي الشبكات أو من يحاولون اختراقها، ومراقبة الشبكة، وتطبيق IDS/IPS الخ).

أ س 346 مختبر حماية شبكات الحاسوب
المتطلب السابق: أ س 345 (أو متزامن)

1 س.م = (0نظري، 3 عملي)

هذا المساق عبارة عن تطبيق عملي يغطي موضوعات أمان الشبكة والنظام. يتضمن المساق دليل شامل لكيفية عمل الإعدادات. ينقسم المساق لقسمين أساسيين وهما أمان الشبكة وأمن نقاط النهاية. سيتمكن الطلاب من فهم كيفية الحصول على شبكات ونقطة النهاية الأمانة وكيفية تصميمها، وتكوين أجهزة الشبكة مثل المفاتيح، وإلقاء نظرة على التكوين الآمن لجدران الحماية، وتصفح الويب والحماية المتقدمة من البرامج الضارة. سيتم تدريس هذه الموضوعات بطريقة عملية خطوة بخطوة.

أ س 371 مختبر نظام التشغيل Linux
المتطلب السابق: ع ح 375

1 س.م = (0نظري، 3 عملي)

يغطي هذا المساق بعض موضوعات نظام التشغيل Linux ، مثل نظام الملفات والأوامر والأدوات المساعدة وتحرير النصوص وبرمجة القشرة وأدوات معالجة النصوص.

أ س 381 ادارة المخاطر
المتطلب السابق: أ س 101

3 س.م = (3نظري، 0 عملي)

يناقش هذا المساق كيفية العثور على المخاطر في مصادر المعلومات ومخازنها والتحكم في هذه المخاطر باستخدام أساليب تحديد المخاطر، والتقييم والتحليل، والرقابة. علاوة على ذلك، فإنه يغطي العوامل السلوكية البشرية الضارة التي تضر بنظم المعلومات.

أ س 391 التدريب الميداني
المتطلب السابق: انتهاء 90 س.م بنجاح

3 س.م = (0نظري، 0 عملي)

يوفر هذا المساق للطلاب فرصة لتجربة بيئة العمل قبل التخرج. يتعين على الطلاب قضاء مدة معينة مسبقاً كمتدرب في مؤسسة معتمدة من قبل قسم الامن السيبراني. خلال هذه الفترة يحتاج الطلاب إلى الانخراط في ممارسات الأمن السيبراني مع مشرفيهم ومراقبة وتجربة أدوار الأمن السيبراني في هذه المؤسسات.

أ س 411 هندسة البرمجيات العكسية
المتطلب السابق: أ س 101، أ س 111، أ س 211

2 س.م = (0نظري، 6 عملي)

يهدف هذا المساق لمساعدة الطلاب بفهم وتحليل البرامج الضارة، واستنتاج كيفية عملها، والمساعدة في التحليل عبر التقنيك. سيتمكن الطلاب من استخدام الأدوات (Ollydbg ، IDAPro) لإجراء تحليل ثابت وديناميكي للبرامج الضارة بأمان، بما في ذلك البرامج المشفرة والمعبأة والمبهمه. على وجه الخصوص، سيكون للمساق مختبرات عملية مكثفة في كل وحدة معرفية.

أ س 412 برمجة تطبيقات المحمول
المتطلب السابق: ع ح 112

3 س.م = (0نظري، 9 عملي)

أصبحت أجهزة الحوسبة المتنقلة في كل مكان. يركز هذا المساق على تطوير حلول الأجهزة المحمولة لمختلف المنصات الحديثة، بما في ذلك أنظمة تشغيل الهواتف المحمولة الرئيسية مثل Android و iOS. كذلك، يتناول هذا المساق موضوعات مختلفة مثل معمارية الأجهزة المحمولة، ولغات البرمجة، وهندسة البرمجيات، وتصميم واجهة المستخدم، وتطبيقات RESTful و Non-RESTful، وإنشاء ودمج خدمات الويب / السحابة، وأجهزة الاستشعار المحمولة، وإدارة الأمان والثقة.

3 س.م = (3نظري، 0 عملي)

أ س 451 أمن البرمجيات

المتطلب السابق: أ س 344+211+452 (أو مترامن)

يقدم هذا المساق المبادئ النظرية والعملية لحماية البرمجيات، مع التركيز على بعض المخاطر التي تواجهها البرمجيات والتي قد تتضمن مشكلة فيضان البيانات، مشكلة اعتماد المخرجات على تسلسل المدخلات، عملية توليد الأرقام العشوائية. كما يركز على تحديد التهديدات ونقاط الضعف التي قد تواجه البرمجيات خلال عملية البناء والتأسيس. وسيتم التركيز على الطرق التي يمكن من خلالها تلافي المشاكل التي سبق ذكرها. كما سيتم التركيز أيضاً على كيفية بناء البرمجيات مع التفكير بمبدأ حمايتها ابتداء من المراحل الأولى لبنائها وحتى المراحل النهائية لعملية البناء.

3 س.م = (2نظري، 3 عملي)

أ س 451 أمن البيانات التحليلي

المتطلب السابق: أ س 343، أ س 371، أ س 111

يهدف هذا المساق إلى مراقبة الشبكات وتوثيقها، وتأمين الشبكات، وإحباط عمل البرامج الضارة، وكذلك منع الاختراقات من خلال تحسين فهم بيئة المعلومات ومعرفة تفاصيلها، واستخدام البيانات وتحليلها لتعزيز أمن أنظمة المعلومات وموجوداتها. وكذلك، يغطي المساق موضوعات مثل كيفية مراقبة شبكات الكمبيوتر، والحصول على البيانات الأمنية وإعدادها، وربط الأحداث الأمنية، واستخدام الأساليب الإحصائية البسيطة لاكتشاف البرامج الضارة والتنبؤ بالسلوكيات المشبوهة. علاوة على ذلك، يحتوي هذا المساق على مجموعة من التجارب العملية التي توفر خبرة عملية في هذا الموضوع.

3 س.م = (2نظري، 3 عملي)

أ س 452 أمن الويب

المتطلب السابق: أ س 343 أو مترامن، ن م 201، ن م 221

يهدف هذا المساق لمساعدة الطلاب بفهم كيفية إنشاء تطبيقات ويب آمنة. يغطي المساق المفاهيم الأساسية لبرمجة الويب، واستغلال نقاط الضعف على الويب، وعيوب تصميم متصفح الويب، وبعض الموضوعات المتقدمة في خصوصية الويب وأمن التجارة الإلكترونية. علاوة على ذلك، سيكون من ضمن المساق مجموعة من التجارب العملية التي توفر خبرة عملية في هذا المجال.

3 س.م = (3نظري، 0 عملي)

أ س 453 أمن الحوسبة السحابية

المتطلب السابق: أ س 452

يهدف هذا المساق لوصف البنية الأمنية السحابية واستكشاف مبادئ تصميم الأمان الإرشادية وأنماط التصميم ومعايير الصناعة والتقنيات المطبقة ومعالجة متطلبات الامتثال التنظيمي الحاسمة لتصميم وتنفيذ وتقديم وإدارة الخدمات السحابية الآمنة. يتعمق المساق في الجوانب المعمارية السحابية الآمنة فيما يتعلق بتحديد المخاطر وتخفيفها، وحماية وعزل البنى التحتية بما في ذلك الحوسبة والشبكة والتخزين وحماية البيانات والمراقبة والتدقيق وتلبية الامتثال لقواعد الصناعة والتفويضات التنظيمية. سيبين المساق الدور الإيجابي لإرشادات الأمان الحوسبة السحابية التي حددتها ISO و NIST و ENISA و Cloud Security Alliance (CSA).

3 س.م = (3نظري، 0 عملي)

أ س 454 أمن إنترنت الأشياء

المتطلب السابق: أ س 343

يغطي هذا المساق المكونات الأساسية لإنترنت الأشياء وكيفية جمع البيانات وتحليلها من أجهزة الاستشعار. علاوة على ذلك، يناقش هذا المساق قضايا الأمن وحلول إنترنت الأشياء، ويشرح التهديدات المختلفة لمنصات إنترنت الأشياء ويعلم الطلاب كيفية الدفاع عن أجهزة إنترنت الأشياء بشكل آمن.

أ س 455 أمن وخصوصية المعلومات الصحية
المتطلب السابق: أ س 101

3 س.م = (3نظري، 0 عملي)

يغطي هذا المساق عدة مواضيع مثل مقدمة إلى الخصوصية وأمن أنظمة معلومات الرعاية الصحية، وكيفية حماية سرية معلومات المريض، وأنواع الوصول المناسب لمعلومات الرعاية الصحية لمقدمي الرعاية الصحية، وناقش كيفية الحد من الوصول غير المصرح به لمعلومات المريض. علاوة على ذلك، يناقش هذا المساق المواصفات والمقاييس التي تساعد في الحفاظ على المعلومات الطبية للمرضى آمنة في بيئة إلكترونية، والقضايا الشائعة لحماية البيانات، وتبادل المعلومات السريرية بين مؤسسات الرعاية الصحية. وكذلك سيتم دراسة قضايا حقيقة متعلقة بأمن المعلومات الصحية واسناد تحليلها للطلاب كمشروع للمساق.

أ س 456 التعلم العميق
المتطلب السابق: ع ح 362

3 س.م = (3نظري، 0 عملي)

يتضمن هذا المساق المبادئ والمفاهيم الأساسية في التعلم العميق. حيث يغطي المساق الموضوعات التالية: النماذج الرياضية والجوانب النظرية لتعلم الآلة وتعلم الخواص والشبكات العصبية الاصطناعية وموضوعات حديثة في علم الذكاء الاصطناعي، مثل ادراج النموذج وإدراك الصوت ومعالجة اللغات الطبيعية.

أ س 461 مقدمة الى علم اخفاء المعلومات
المتطلب السابق: أ س 261

3 س.م = (2نظري، 3 عملي)

هذا المساق يقدم اساسيات موارد المعلومات. يغطي مبادئ الموارد الرقمية وتحليلها، الدمج الرقمي متضمناً خوارزميات إخفاء المعلومات في وسائل مختلفة مثل ملفات الصور، الصوت، والفيديو. هذا المساق يشمل مقدمة لأدوات معروفة لإخفاء وكشف المعلومات. يتضمن هذا المساق مجموعة من التجارب التطبيقية تهدف لتوفير خبرة عملية في هذا المجال.

أ س 462 نظرية التشفير المتقدمة
المتطلب السابق: أ س 261

3 س.م = (3نظري، 0 عملي)

يغطي هذه المساق موضوعات متقدمة في علم التشفير مثل البروتوكولات المتقدمة (البراهين في حالة المعرفة الصفرية، والبروتوكولات، ومشاركة الاسرار)، والتشفير متماثل الشكل بالكامل، والتعتيم والتشفير الكمي.

أ س 471 أمن نظم التشغيل
المتطلب السابق: أ س 261، أ س 371

3 س.م = (2نظري، 3 عملي)

يقدم هذا المساق اساسيات امن نظم التشغيل من خلال تغطية آليات السيطرة على الوصول للمعلومات، حماية الذاكرة، وآليات وسياسات الحماية على مستوى نظام التشغيل (برمجياً او معداتياً) والتي تهدف للتصدي للهجمات الامنية مثل الـ malware. يشمل هذا المساق مبادئ الانظمة (الألات) الافتراضية واستخداماتها في فهم وتحليل نظم التشغيل الحديثة (بما فيها انظمة تشغيل الاجهزة المحمولة) من اجل تحديد المخاطر المتعلقة بأنظمة التشغيل. يتضمن هذا المساق مجموعة من التجارب التطبيقية تهدف لتوفير خبرة عملية في هذا المجال.

أس 481 الاختراق الأخلاقي (1)

3 س.م = (1نظري، 6 عملي)

المتطلب السابق: أس 344

يغطي هذا المساق أخلاقيات وقوانين القرصنة الأخلاقية، ويناقش أنواع التهديدات المختلفة بما في ذلك التهديد الصادر من داخل المؤسسات مثل التهديد الصادر من الموظفين. علاوة على ذلك، فإنه يشرح الأساليب التي يستخدمها المتسلل الأخلاقي كالاستطلاع وجمع المعلومات، واستكشاف الشبكات وكيفية الولوج إليها، وجمع معلومات تفصيلية عن الانظمة المستهدفة وبرامجها، وتحليل الثغرات الأمنية وصولاً إلى اختراق النظام. يتكون هذا المساق من مجموعة من التجارب العملية التي توفر خبرة عملية في القرصنة الأخلاقية.

أس 482 الاختراق الأخلاقي (2)

3 س.م = (0نظري، 9 عملي)

المتطلب السابق: أس 452، أس 481

يناقش هذا المساق موضوعات متقدمة في القرصنة الأخلاقية، ويتكون من تجارب عملية متقدمة مثل تهديدات البرامج الضارة والتحليل، والتجسس على المعلومات المرسلّة من خلال شبكات الكمبيوتر، واستعمال المهارات الاجتماعية للحصول على المعلومات بطريقة غير شرعية، وتعطيل خدمات أنظمة المعلومات، والولوج إلى أنظمة المعلومات من خلال السيطرة على قنوات الاتصال الشرعية بطريقة غير شرعية، والتهرب من الإجراءات الأمنية المضادة، واختراق خوادم وتطبيقات الويب، واختراق أنظمة قواعد البيانات من خلال ارسال استعلامات غير شرعية، واختراق الشبكات اللاسلكية واختراق منصات الهواتف المحمولة واختراق إنترنت الأشياء. علاوة على ذلك، يتكون هذا المساق من مجموعة من التجارب العملية التي توفر خبرة عملية في هذا الموضوع.

أس 483 التحقيق الجنائي الرقمي

2 س.م = (2نظري، 0 عملي)

المتطلب السابق: أس 451، أس 411

يقدم هذا المساق معرفة نظرية وتطبيقية عن مبادئ وممارسات التحقيقات الرقمية. يغطي هذا المساق مصادر الأدلة الرقمية، التحقيق الرقمي، وإساليب التحليل الرقمي. تشمل مواضيع هذا المساق فحص ذاكرة الحاسوب واسترجاعها وتحليل السجلات الرقمية، كما يتضمن المساق تحليل سجل النظام، البريد الإلكتروني وقواعد البيانات.

أس 484 مختبر التحقيق الجنائي الرقمي

1 س.م = (0نظري، 3 عملي)

المتطلب السابق: أس 483 أو متزامن

يعطي هذا المساق خبرة عملية تطبيقية على مجموعة من ادوات التحليل الرقمي السائدة من خلال تغطية وظائف هذه الادوات والنظريات التي تعتمد عليها والمقارنة فيما بينها.

أس 485 طرق منهجية في الأمن السيبراني

3 س.م = (3نظري، 0 عملي)

المتطلب السابق: أس 261

يقدم هذا المساق تطبيقات الأساليب المنهجية (الرياضية والمنطقية) في الأمن السيبراني. يركز هذا المساق على التوصيف المنهجي لبروتوكولات الأمن السيبراني باستخدام لغات معرفة رياضياً مثل SPS، AVISPA IF، و π -calculus ومن ثم إجراء تحقق منهجي لهذه البروتوكولات باستخدام ادوات التحقق السائدة مثل OFMC و Proverif.

أس 491 مشروع التخرج (1)

1 س.م = (1نظري، 0 عملي)

المتطلب السابق: انتهاء 90 ساعة بنجاح

تتيح هذه المادة للطالب فرصة إعداد مشروع تخرج جوهري تحت إشراف عضو هيئة تدريس. وعلى الطالب أن يتقدم لرئيس القسم قبل التسجيل بأسبوعين بطلب مكتوب للسماح بتنفيذ مشروع تخرج يتم تحديد معالمه الأولية والمشرف على تنفيذه. ويقوم الطالب من خلال هذه المادة بتحديد متطلبات وتصميم النظام أو البرمجية المقترحة.

أ س 492 التخرج (2)

2 س.م = (2 نظري، 0 عملي)

المتطلب السابق: أ س 491 .

هذا المساق استمرار للمساق "أ س 491"، ويقوم الطالب فيه ببناء وفحص النظام أو البرمجية المقترحة في مشروع التخرج (1)، ويقدم المشروع المكتمل وتقريراً مكتوباً عنه للجنة فحص ثلاثية يكون المشرف رئيسها، كما ويقدم الطالب نسخة من التقرير للقسم.

أ س 493-أ موضوعات خاصة في الأمن السيبراني (1)

3 س.م = (3 نظري، 0 عملي)

المتطلب السابق: موافقة القسم

يختار القسم موضوعاً يتعلق بمجال الأمن السيبراني.

أ س 493-ب موضوعات خاصة في الأمن السيبراني (2)

3 س.م = (3 نظري، 0 عملي)

المتطلب السابق: موافقة القسم

يختار القسم موضوعاً يتعلق بمجال الأمن السيبراني.