СИЛЛАБУС
2023-2024 оқу жылының көктемгі семестрі
«Ақпараттық жүйелер» білім беру бағдарламасы

ID және Пәннің атауы	Білім алушының өзіндік жұмысын (СӨЖ)	Кредит саны			Кредит-тердің жалпы саны	Оқытушының жетекшілігімен білім алушының өзіндік жұмысы (СОӨЖ)
		Дәрістер (Д)	Семинарс абақтар (ПС)	Зерт. сабақтар (ЗС)		
77641 Операциялық жүйелер қауіпсізді	2	15	-	30	5	7

ПӘН ТУРАЛЫ АКАДЕМИЯЛЫҚ АҚПАРАТ

Оқытудың түрі	Курстың типі/сипаты	Дәріс түрлері	Семинар сабақтардың түрлері	Қорытынды бақылаудың түрі мен платфомасы
Оффлайн	БП, ТК компоненті	Теориялық	Зертханалық сабақтар	Дәстүрлі жазбаша, оффлайн
Дәріскер	Мағазов Райымбек Саламатұлы			
e-mail:	magazovraiko@gmail.com			
Телефон:	+77759150722 (только Whatsapp)			
Ассистенттер:	Қалидоллина Гүлмаржан Талғатқызы Байсылбаева Кымбат Данияровна Кенжебаева Мерей Омаровна Байкувеков Мейржан Берикович			
e-mail:	kalidollina2021@gmail.com baisylbaeva.k@gmail.com merey-mex-2017@mail.ru (Мерей Омаровна) baikuvekov@gmail.com			
Телефон:	87058047455 (Қалидоллина Гүлмаржан) 87772797997 (Байсылбаева Қымбат) 87785090132 (Мерей Омаровна) 87026478122 (Байкувеков Мейржан)			

ПӘННІҢ АКАДЕМИЯЛЫҚ ПРЕЗЕНТАЦИЯСЫ

Пәннің мақсаты	Оқытудың күтілетін нәтижелері (ОН)*	ОН қол жеткізу индикаторлары (ЖИ)
Пәннің мақсаты: қауіпсіздік функцияларын және жалпы операциялық жүйелердің функцияларын қолдану қабілетін қалыптастыру. Келесілер қарастырылады: Операциялық жүйелерді құру принциптері; Бағдарламалық құралдардың жіктелуі; Операциялық жүйелердің жіктелуі; Операциялық жүйелердің тұжырымдамалы	1. Әр түрлі әдістер мен құралдарды қолдана отырып, операциялық жүйелердің ағымдағы қауіпсіздік деңгейін талдау және бағалау. Бұл жүйенің конфигурациясына, белсенді қызметтерге және қауіпсіздік параметрлеріне негізделген осалдықтар мен тәуекелдерді анықтау мүмкіндігін қамтиды.	1.1 Жүйе конфигурациясындағы осалдықтар мен әлсіз жақтарды анықтайды және құжаттайды.
		1.2 Қауіпсіздік көрсеткіштері мен рейтингтері арқылы қауіпсіздік шараларының тиімділігін бағалайды.
	2. Windows және Linux операциялық жүйелерінде пайдаланушыларды және кіру құқықтарын басқару үшін қауіпсіздік принциптерін іс жүзінде қолданыңыз. Бұл есептік жазбаларды құру мен басқаруды, сондай-ақ пайдаланушылар мен топтардың кіру құқықтарын орнатуды және басқаруды қамтиды	2.1 Пайдаланушы тіркелгілерін және кіру құқығын орнататын топтарды жасайды және басқарады.
		2.2 Пайдаланушылардың жүйелік ресурстарға қол жетімділігін шектеу үшін қауіпсіздік саясатын орнатады және қолданады.
	3. Windows және Linux операциялық жүйелерінде пайдаланушыларды және кіру құқықтарын басқару үшін қауіпсіздік принциптерін іс жүзінде қолданыңыз. Бұл есептік жазбаларды құру мен басқаруды, сондай-ақ пайдаланушылар мен топтардың кіру құқықтарын орнатуды және басқаруды қамтиды	3.1 Зиянды бағдарламаны анықтау және бұғаттау үшін антивирустық бағдарламалық жасақтаманы конфигурациялайды және басқарады.
		3.2 Желі мен ресурстарды қорғау үшін брандмауэрлер мен кіруді анықтау жүйелерін конфигурациялайды.
	4. PAM (Pluggable Authentication Module) және Active Directory топтық саясаты негізінде қауіпсіздік саясатын жобалау және іске асыру. Бұл аутентификация және авторизация әдістерін әзірлеу мен конфигурациялауды,	4.1 Қол жетімділікті шектеу және аутентификацияны күшейту үшін PAM қауіпсіздік саясатын жасайды және қолданады.

		4.2 Деректерді ұстауға немесе өзгертуге мүмкіндік беретін деректерді тасымалдау процесінің осал тұстарын анықтайды.
	5. Қауіпсіздік инциденттерін анықтайды және оларға жауап береді, соның ішінде инциденттерге әрекет ету жоспарларын әзірлеу, инциденттерден кейін талдау жүргізу және болашақ қауіптердің алдын алу үшін қажетті шараларды қабылдайды.	5.1 Қауіпсіздік оқиғаларын басқару, тергеу және жою қадамдарын сипаттайтын оқиғаларға жауап беру жоспарларын әзірлейді.
		5.2 Себептерді анықтау, әсерлерді бағалау және болашақта ұқсас оқиғалардың алдын алу шараларын әзірлеу үшін оқиғадан кейінгі талдауды жүргізеді.
Пререквизиты	Ақпараттық қауіпсіздік негіздері	
Постреквизиты	Киберқауіпсіздік	
Әдебиет және ресурстар	**Оқу әдебиеттері:** 1. Пракхар, П. (2018). "Современное тестирование безопасности веб-приложений." Питер. 2. Яворски, П. (2020). "Веб-хакинг 101." БХВ-Петербург.Введение в веб-хакинг с примерами реальных уязвимостей и методов их эксплуатации. 3. OWASP Foundation. (2020). "OWASP Testing Guide v4." Open Web Application Security Project.Практическое руководство по тестированию безопасности веб-приложений, охватывающее все аспекты веб-безопасности. 4. Sagar Rahalkar, (2021) .A Complete Guide to Burp Suite: Learn to Detect Application Vulnerabilities **Қосымша әдебиеттер:** 1. **Макдональд, М. (2020). "Безопасность веб-разработки: реальные угрозы, практическая защита." ДМК Пресс.**Практическое руководство для веб-разработчиков о важных аспектах веб-безопасности. 2. **Эриксон, Дж. (2008). "Искусство эксплуатации." Питер.**Обширное изложение принципов хакинга и эксплуатации, полезное для понимания методов атак и защиты **Интернет-ресурстар:** 1. https://portswigger.net/web-security 2. https://hackthebox.com 3. https://github.com/JohnHammond 4. https://www.youtube.com/johnhammond010 5. https://www.root-me.org/ru/ 6. https://www.vulnhub.com/ Қосымша оқу материалдар, сондай-ақ үй тапсырмалары мен жобаларды орындау үшін univer.kaznu.kz сайтыңыздағы ПОӘК бөлімінде қолжетімді болады.	

Пәннің академиялық саясаты	Пәннің академиялық саясаты Әл-Фараби атындағы ҚазҰУ-дың Академиялық саясатымен және академиялық адалдық саясатымен айқындалады. Құжаттар Univer АЖ басты бетінде қолжетімді. **Ғылым мен білімнің интеграциясы.** Студенттердің, магистранттардың және докоранттардың ғылыми-зерттеу жұмысы – бұл оқу үдерісінің тереңдетілуі. Ол тікелей кафедраларда, зертханаларда, университеттің ғылыми және жобалау бөлімшелерінде, студенттік ғылыми-техникалық бірлестіктерінде ұйымдастырылады. Білім берудің барлық деңгейлеріндегі білім алушылардың өзіндік жұмысы заманауи ғылыми-зерттеу және ақпараттық технологияларды қолдана отырып, жаңа білім алу негізінде зерттеу дағдылары мен құзыреттіліктерін дамытуға бағытталған. Зерттеу университетінің оқытушысы ғылыми-зерттеу қызметінің нәтижелерін дәрістер мен семинарлық (практикалық) сабақтар, зертханалық сабақтар тақырыбында, силлабустарда көрініс табатын және оқу сабақтары мен тапсырмалар тақырыптарының өзектілігіне жауап беретін **СОӨЖ, СӨЖ** тапсырмаларына біріктіреді. **Сабаққа қатысуы.** Әр тапсырманың мерзімі пән мазмұнын іске асыру күнтізбесінде (кестесінде) көрсетілген. Мерзімдерді сақтамау баллдардың жоғалуына әкеледі. **Академиялық адалдық.** Практикалық/зертханалық сабақтар, БӨЖ білім алушының дербестігін, сыни ойлауын, шығармашылығын дамытады. Плагиат, жалғандық, шпаргалка пайдалану, тапсырмаларды орындаудың барлық кезеңдерінде көшіруге жол берілмейді. Теориялық оқыту кезеңінде және емтихандарда академиялық адалдықты сақтау негізгі саясаттардан басқа «Қорытынды бақылауды жүргізу Ережелері», «Ағымдағы оқу жылының күзгі/көктемгі семестрінің қорытынды бақылауын жүргізуге арналған Нұсқаулықтары», «Білім алушылардың тестілік құжаттарының көшіріліп алынуын тексеру туралы Ережесі» тәрізді құжаттармен регламенттеледі. **Инклюзивті білім берудің негізгі принциптері.** Университеттің білім беру ортасы гендерлік, нәсілдік/этникалық тегіне, діни сенімдеріне, әлеуметтік-экономикалық мәртебесіне, студенттің

	физикалық денсаулығына және т.б. қарамастан, оқытушы тарапынан барлық білім алушыларға және білім алушылардың бір-біріне әрқашан қолдау мен тең қарым-қатынас болатын қауіпсіз орын ретінде ойластырылған. Барлық адамдар құрдастары мен курстастарының қолдауы мен достығына мұқтаж. Барлық студенттер үшін жетістікке жету, мүмкін емес нәрселерден гөрі не істей алатындығы болып табылады. Әртүрлілік өмірдің барлық жақтарын күшейтеді. Барлық білім алушылар, әсіресе мүмкіндігі шектеулі жандар, телефон +77759150722 (Whatsapp) немесе MS Teams-тегі бейне байланыс арқылы *https://teams.microsoft.com/l/team/19%3aUcFTo9piWXY0jssU0pecnG4Pqc1385iR-nAziICYffM1%40thread.tacv2/conversations?groupId=f170a507-0551-473d-bc30-4d3f8d0c7ba5&tenantId=b0ab71a5-75b1-4d65-81f7-f479b4978d7b.* кеңестік көмек ала алады. **MOOC интеграциясы (massive openlline course). MOOC**-тың пәнге интеграциялануы жағдайында барлық білім алушылар **MOOC**-қа тіркелуі қажет. **MOOC** модульдерінің өту мерзімі пәнді оқу кестесіне сәйкес қатаң сақталуы керек. **Назар салыңыз!** Әр тапсырманың мерзімі пәннің мазмұнын іске асыру күнтізбесінде (кестесінде) көрсетілген, сондай-ақ **MOOC**-та көрсетілген. Мерзімдерді сақтамау баллдардың жоғалуына әкеледі.

ОҚЫТУ ТУРАЛЫ АҚПАРАТ, ОҚЫТУ ЖӘНЕ БАҒАЛАУ

Оқу жетістіктерін есепке алуды бағалаудың балдық-рейтингтік әріптік жүйесі

Бағалау	Ұпайларды ң сандық баламасы	Ұпайлар, % мазмұны	Дәстүрлі жүйе бойынша бағалау
A	4,0	95-100	Өте жақсы
A-	3,67	90-94	
B+	3,33	85-89	жақсы
B	3,0	80-84	
B-	2,67	75-79	
C+	2,33	70-74	
C	2,0	65-69	Қанағаттанарлық
C-	1,67	60-64	
D+	1,33	55-59	
FX	0.5	25-49	Қанағаттанарлықсыз
F	0	0-24	

Бағалау әдістері

Критериалды бағалау – нақты әзірленген критерийлер негізінде оқытудың нақты қол жеткізілген нәтижелерін оқытудың күтілетін нәтижелерімен салыстыру процесі. Формативті және жиынтық бағалауға негізделген.

Формативті бағалау – күнделікті оқу қызметі барысында жүргізілетін бағалау түрі. Ағымдағы көрсеткіш болып табылады. Білім алушы мен оқытушы арасындағы жедел өзара байланысты қамтамасыз етеді. Білім алушының мүмкіндіктерін анықтауға, қиындықтарды анықтауға, ең жақсы нәтижелерге қол жеткізуге көмектесуге, оқытушының білім беру процесін уақтылы түзетуге мүмкіндік береді. Дәрістер, семинарлар, практикалық сабақтар (пікірталастар, викториналар, пікірталастар, дөңгелек үстелдер, зертханалық жұмыстар және т.б.) кезінде тапсырмалардың орындалуы, аудиториядағы жұмыс белсенділігі бағаланады. Алынған білім мен құзыреттілік бағаланады.

Жиынтық бағалау - пән бағдарламасына сәйкес бөлімді зерделеу аяқталғаннан кейін жүргізілетін бағалау түрі. СРО орындаған кезде семестрде 3-4 рет өткізіледі. Бұл оқытудың күтілетін нәтижелерін дескрипторлармен арақатынаста игеруді бағалау. Белгілі бір кезеңдегі пәнді меңгеру деңгейін анықтауға және тіркеуге мүмкіндік береді. Оқу нәтижелері бағаланады.

Формативті және жиынтық бағалау	Ұпайлар % мазмұны
Зертханалық сабақтарда жұмыс істеу	20
Өзіндік жұмыс	30
Жобалық және шығармашылық қызмет	10
Қорытынды бақылау (емтихан)	40
ҚОРЫТЫНДЫ	100

Оқу курсының мазмұнын жүзеге асыру күнтізбесі (кестесі). Оқыту және оқыту әдістері.

Апта	Тақырып атауы	Сағат саны	Макс. балл***
	Модуль 1 Веб Қауіпсіздік Негіздері		
1	**Д1.** Веб-қауіпсіздік пәніне кіріспе.	1	
	ЗС1. PortSwigger жүйесіне тіркелу және зертханалық дайындық	2	7
2	**Д2.** Веб-ресурстарға шабуыл жасау әдістері	1	
	ЗС2. Burpsuite құралдарын орнату және таныстыру	2	7
	СӨЖ 1. Web осалдығы тақырыбында СӨЖ1 орындау бойынша кеңес беру	1	
3	**Д3.** BurpSuite тестілеу бағдарламасына кіріспе	1	
	ЗС3. PortSwigger Academy labs. Dom XSS зертханасынан өту	2	7
	Веб-ресурстардың осалдығы. DVWA	1	20
4	**Д4.** XSS және CSRF-ті түсіну және қорғау.	1	
	ЗС4. PortSwigger Academy labs. Dom XSS 2 зертханасынан өту	2	7
	СӨЖ 2. Коллоквиум	1	11
5	**Д5.** SQL инъекцияларынан қорғау түрлері мен әдістері.	1	
	ЗС5. PortSwigger Academy labs. Жасырын деректерді алуға мүмкіндік беретін WHERE сөйлеміндегі SQL инъекциясының осалдығы.	2	7
	Модуль 2 Сервер қауіпсіздігі және API қорғау әдістері		
6	**Д6.** SQL инъекциясы -1. UNION-SQL инъекциялық шабуылдары	1	

	ЗС6. PortSwigger Academy labs. Жүйеге кіруді айналып өту үшін SQL инъекциясының осалдығы	**2**	**7**
	СОӨЖ 3. СӨЖ 2 орындау бойынша Консультация.	**1**	
7	**Д7.** SQL инъекциясы -2. SQL инъекциялық шабуылдар үшін дерекқорды тексеру	**1**	
	ЗС7. PortSwigger Academy labs. Сұрау арқылы қайтарылған бағандар санын анықтайтын UNION SQL инъекциялық шабуылы	**2**	**7**
	СӨЖ 2. CTF тапсырмаларына негізделген Квест.	**1**	**20**
АБ 1			**100**
8	**Д8.** Аутентификация және сессияны басқару	**1**	
	ЗС8. PortSwigger Academy labs. Қауіпсіз аутентификация	**2**	**6**
	СОӨЖ 4. Коллоквиум	**1**	**6**
9	**Д9.** Сервер қауіпсіздігінің конфигурациясы, файлдық жүйені қорғау.	**1**	
	ЗС9. PortSwigger Academy labs. Сервер қауіпсіздігін талдау және күшейту.	**2**	**6**
	СОӨЖ 5. СӨЖ 3 орындау бойынша Консультация.		
10	**Д10.** API және микросервистерді қорғау	**1**	
	ЗС10. PortSwigger Academy labs. API тестілеу.	**2**	**6**
	СӨЖ 3. CTF тапсырмаларына негізделген Квест.	**1**	**20**
Модуль 3 Веб қосымшаның аудиті			
11	**Д11.** Сайтаралық сұрауды жалған жасау (CSRF)	**1**	
	ЗС11. PortSwigger Academy labs. CSRF қорғалмаған осалдығы	**2**	**6**
12	**Д12.** Сайтаралық сценарий XSS	**1**	
	ЗС12. PortSwigger Academy labs. XSS кодтаусыз	**2**	**6**
	СОӨЖ 6. СӨЖ 4 орындау бойынша Консультация.	**1**	**6**
13	**Д13.** XML сыртқы нысанды ендіру (XXE)	**1**	
	ЗС13. PortSwigger Academy labs. Файлдарды шығарып алу үшін сыртқы нысандарды пайдаланып XXE пайдалану	**2**	**6**
	СӨЖ 4. CTF тапсырмаларына негізделген Квест.	**1**	**20**
14	**Д14.** Сервер тарапынан сұрауды жалған жасау (SSRF)	**1**	
	ЗС14. PortSwigger Academy labs. SSRF шабуылдарын орындау үшін XXE пайдалану	**2**	**6**
15	**Д15.** Жетілдірілген осалдықтар мен шабуылдар	**1**	
	ЗС15. PortSwigger Academy labs. PortSwigger қиын тапсырмаларында тәжірибе.	**2**	**6**
	СОӨЖ 7. Емтихан сұрақтарына дайындық бойынша кеңес беру.		
АБ 2			**100**

ЖИЫНТЫҚ БАҒАЛАУ РУБРИКАТОРЫ
ОҚУ НӘТИЖЕЛЕРІН БАҒАЛАУ КРИТЕРИЙЛЕРІ

СӨЖ 1. Веб-ресурстардың осалдығы. DVWA" (100% аралық бақылаудың 20%-ы)

Критерий	«Өте жақсы» 15-20 %	«Жақсы» 10-15%	«Қанағаттанарлық» 5-10%	«Қанағаттанарлықсыз» 0-5%
Ақпараттық қауіпсіздік аудитінің техникалық процедураларының теориялары мен тұжырымдамаларын түсіну	**Веб-қауіпсіздіктің** теорияларын, тұжырымдамаларын терең түсіну. Тиісті және нормативтік құжаттар мен негізгі көздер ұсынылады.	**Веб-қауіпсіздіктің** теорияларын, тұжырымдамаларын түсіну. Тиісті және нормативтік құжаттар мен негізгі көздер ұсынылады.	**Веб-қауіпсіздіктің** теорияларын, тұжырымдамаларын шектеулі түсіну. Тиісті және нормативтік құжаттар мен негізгі көздер ұсынылады.	**Веб-қауіпсіздіктің** теорияларын, тұжырымдамаларын үстірт түсіну/ түсінбеушілік. Тиісті және нормативтік құжаттар мен негізгі көздер ұсынылмайды.
Қазақстандағы ақпараттық қауіпсіздік аудитінің негізгі мәселелерін түсіну	**Веб-қауіпсіздікті** жүргізу рәсімдерінің негізгі ұғымдарын жақсы байланыстырады. Негізгі көздерді қолданады. Дәлелдерді эмпирикалық зерттеудің дәлелдерімен тамаша негіздеу (мысалы, аудиторлық бағдарламаларды немесе статистикалық талдауды қолдану негізінде).	**Веб-қауіпсіздікті** жүргізу рәсімдерінің негізгі ұғымдарын байланыстырады. Арнайы бағдарламалық жасақтамаға иелік ету арқылы дәлелдерді күшейтеді	**Веб-қауіпсіздікті** жүргізу жөніндегі тұжырымдамалардың шектеулі байланысы. Эмпирикалық зерттеу дәлелдерін шектеулі қолдану.	**Веб-қауіпсіздікті** жүргізу тұжырымдамаларының шамалы немесе байланысы жоқ. Бағдарламалық жасақтаманы аз немесе мүлдем пайдаланбайды.
Қойылған міндеттерді шешу	**Веб-қауіпсіздікті** жүргізу бойынша сауатты практикалық шешімдерді ұсынады	**Веб-қауіпсіздікті** жүргізу бойынша кейбір практикалық шешімдерді ұсынады	Шешімдер маңызды емес, мұқият талдауға негізделмеген және таяз.	**Веб-қауіпсіздік** бойынша шешім аз немесе мүлдем жоқ
Шешімдерді рәсімдеу және ұсыну	Жазу айқындықты, нақтылықты және дұрыстығын көрсетеді.	Жазу айқындықты, нақтылықты және дұрыстығын көрсетеді.	Хатта кейбір негізгі қателер бар және анықтықты жақсартып жазу қажет.	Түсініксіз жазылған, мазмұнын ұғу, түсіну қиынға соғады.

CTF тапсырмаларына негізделген Квест (100% аралық бақылаудың 20%-ы)

Критерий	«Өте жақсы» 15-20 %	«Жақсы» 10-15%	«Қанағаттанарлық» 5-10%	«Қанағаттанарлықсыз» 0-5%
Ақпараттық қауіпсіздік аудитінің техникалық процедураларының теориялары мен тұжырымдамаларын түсіну	**Веб-қауіпсіздіктің теорияларын, тұжырымдамаларын терең түсіну. Тиісті және нормативтік құжаттар мен негізгі көздер ұсынылады.**	**Веб-қауіпсіздіктің теорияларын, тұжырымдамаларын түсіну. Тиісті және нормативтік құжаттар мен негізгі көздер ұсынылады.**	**Веб-қауіпсіздіктің теорияларын, тұжырымдамаларын шектеулі түсіну. Тиісті және нормативтік құжаттар мен негізгі көздер ұсынылады.**	**Веб-қауіпсіздіктің теорияларын, тұжырымдамаларын үстірт түсіну/ түсінбеушілік. Тиісті және нормативтік құжаттар мен негізгі көздер ұсынылмайды.**
Қазақстандағы ақпараттық қауіпсіздік аудитінің негізгі мәселелерін түсіну	**Веб-қауіпсіздікті жүргізу рәсімдерінің негізгі ұғымдарын жақсы байланыстырады. Негізгі көздерді қолданады. Дәлелдерді эмпирикалық зерттеудің дәлелдерімен тамаша негіздеу (мысалы, аудиторлық бағдарламаларды немесе статистикалық талдауды қолдану негізінде).**	**Веб-қауіпсіздікті жүргізу рәсімдерінің негізгі ұғымдарын байланыстырады. Арнайы бағдарламалық жасақтамаға иелік ету арқылы дәлелдерді күшейтеді**	**Веб-қауіпсіздікті жүргізу жөніндегі тұжырымдамалардың шектеулі байланысы. Эмпирикалық зерттеу дәлелдерін шектеулі қолдану.**	**Веб-қауіпсіздікті жүргізу тұжырымдамаларының шамалы немесе байланысы жоқ. Бағдарламалық жасақтаманы аз немесе мүлдем пайдаланбайды.**
Қойылған міндеттерді шешу	**Веб-қауіпсіздікті жүргізу бойынша сауатты практикалық шешімдерді ұсынады**	**Веб-қауіпсіздікті жүргізу бойынша кейбір практикалық шешімдерді ұсынады**	Шешімдер маңызды емес, мұқият талдауға негізделмеген және таяз.	**Веб-қауіпсіздік бойынша шешім аз немесе мүлдем жоқ**
Шешімдерді рәсімдеу және ұсыну	Жазу айқындықты, нақтылықты және дұрыстығын көрсетеді.	Жазу айқындықты, нақтылықты және дұрыстығын көрсетеді.	Хатта кейбір негізгі қателер бар және анықтықты жақсартып жазу қажет.	Түсініксіз жазылған, мазмұнын ұғу, түсіну қиынға соғады.

Декан м.а. _____ **Тұрар О.Н.**

Кафедра меңгерушісі _____ **Мусиралиева Ш.Ж.**

Дәріскер _____ **Мағазов Р.С.**