

Әл-Фараби атындағы Қазақ ұлттық университеті
Ақпараттық технологиялар факультеті

СИЛЛАБУС
2020-2021 оқу жылының көктемгі семестрі
«Ақпараттық қауіпсіздік жүйелері» білім беру бағдарламасы

Пәннің коды	Пәннің атауы	Студенттің өзіндік жұмысы (СӨЖ)	Сағат саны			Кредит саны	Студенттің оқытушы басшылығымен өзіндік жұмысы (СОӨЖ)
			Дәрістер (Д)	Практ. сабақтар (ПС)	Зерт. сабақтар (ЗС)		
SB 3302	Желілік қауіпсіздік 2		15	15	15	5	
Курс туралы академиялық ақпарат							
Оқытудың түрі	Курстың типі/сипаты	Дәріс түрлері		Практикалық сабақтардың түрлері	СӨЖ саны	Қорытынды бақылау түрі	
Онлайн / біріктірілген	Теориялық	проблемалы, аналитикалық дәріс		міндеттерді шешу, жағдаяттық тапсырмалар	3-тен кем емес	Универ жүйесінде тест	
Дәріскер	Г.К.Ордабаева, PhD докторант, аға оқытушы					Оф./с.	Сабақ кестесі бойынша
e-mail	gulzi200988@mail.ru						
Телефондары	8-707-932-57-85						

Курстың академиялық презентациясы

Пәннің мақсаты	Оқытудың күтілетін нәтижелері (ОН) Пәнді оқыту нәтижесінде білім алушы қабілетті болады:	ОН қол жеткізу индикаторлары (ЖИ)
Студенттерге заманауи технологиялардағы компьютерлік желілерді пайдалану мен дамытудың маңыздылығын түсіндіру және студенттерді желілер мен телекоммуникациялық жүйелердің жұмыс істеуінің негізгі принциптерімен таныстыру	ОН 1 (когнитивті) - виртуалды машиналарды және желі мониторингінің құралдарын пайдалана білу;	1.1. ену тестілеуінің әдіснамасын негіздеу; 1.2. пакеттік трафикті ұстап алуды және сүзуді сипаттау; 1.3. виртуалды машиналарды орнату талаптарын сипаттау;
	ОН 2 (функционалды) - бағыттау протоколдарының, желілік сүзгілердің параметрлерін қолдануды және виртуалды машиналарда эксперимент жүргізуді игеру;	2.1. ақпарат жинау үшін автоматтандырылған құралдарды қолдану; 2.2. портты сканерлеуді салыстыру; 2.3. виртуалды машиналардың мүмкіндіктерін қолдану;
	ОН 3 (функционалды) - желілер мен телекоммуникациялық жүйелердің, олардың кіші жүйелерінің, тораптары мен буындарының жұмыс қабілеттілігін талдау және болжау;	3.1. пакеттерді талдау үшін командалық жолдың құралдарын тәжірибеде қолдану; 3.2. қызметтік бағдарламалардың мүмкіндіктерін дәлелдеу;
	ОН 4 (жүйелік) - жергілікті желілерді жобалау мен жетілдіруді ұйымдастыру;	4.1. осалдықтарды автоматты түрде қарап шығуды ұйымдастыру; 4.2. парольдерге дербес шабуыл жасау үшін пайдаланылатын құралдарды бағалау;
	ОН 5 (жүйелік) - компьютерлік желілерді бақылаудың кіріктірілген құралдарын пайдалануды ұсыну.	5.1. желілерге енуді тестілеу экспериментін жүргізу; 5.2. веб-қосымшалардағы осалдықтарды анықтауға арналған құралдарды ұсыну;
Пререквизиттер	Желілік қауіпсіздік 1, Компьютерлік желі, Математикалық анализ	
Постреквизиттер	Ақпараттық қауіпсіздіктің нормативті-құқықтық қамтамасыздандыруы, Киберқауіпсіздік, Қауіпсіздікті басқару жүйелері	

Әдебиет және ресурстар	<p>Әдебиеттер: <i>Негізгі:</i> 1. Сандерс, Крис. Анализ пакетов: практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях, 3-е изд.: Пер. с англ. - СПб. : ООО "Диалектика", 2019 - 448 с. : ил. - Парал. тит. англ. 2. Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли. Kali Linux. Тестирование на проникновение и безопасность. — СПб.: Питер, 2020. - 448 с.: ил. — (Серия «Для профессионалов».) 3. Милосердов А.В. Тестирование на проникновение с помощью Kali Linux 2.0. По материалам сайта WebWare.biz, 2015. - 348 с.: ил. 4. Travis Marlette. Splunk Best Practices. Birmingham B3 2PB, UK, 2016. – 238p. 5. Миллер Дж. Д. Implementing Splunk 7. 2018, Packt Publishing – 490p. 6. Uldis Dzerkals. EVE-NG Professional Cookbook. Version 1.4. EVE-NG Limited, 204p.</p> <p><i>Қосымша</i> 1. Uenstrom M. Securing networks Cisco. – М.: Williams, 2015. – 698 p. 2. Анализатор протоколов Wireshark/ П.Н. Толмачев, Н.А. Ермакова, П.В. Подворный, С.А. Сапсай: Учебно-методическое пособие для выполнения лабораторных работ. – М.: РУТ (МИИТ), 2016. – 38 с. 3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. - М.: Форум-Инфра-М, 2013. – 416 с. 4. Justin Hutchens. Kali Linux Network Scanning Cookbook. 2014, Packt Publishing – 452p. 5. Vivek Ramachandran, Cameron Buchanan. Kali Linux Wireless Penetration Testing Beginner's Guide. 2014, Packt Publishing – 214p. 6. Bragg R. Rhodes Owsley M. Strassberg KE Network Security. Complete Guide – М: Economy, 2016. – 312 p. 7. Charit Mishra. Secure your network through protocol analysis. 2018, Packt Publishing – 155p.</p> <p><i>Интернет-ресурстар:</i> 1. https://www.virtualbox.org 2. https://linux.org 3. https://ubuntu.ru 4. https://itskillsup.ru 5. https://www.wireshark.org</p>
------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Университеттік моральдық-этикалық құндылықтар шеңберіндегі курстың академиялық саясаты	<p>Академиялық тәртіп ережелері: Барлық білім алушылар ЖООК-қа тіркелуі қажет. Онлайн курс модульдерін өту мерзімі пәнді оқыту кестесіне сәйкес мұлтіксіз сақталуы тиіс. НАЗАР АУДАРЫҢЫЗ! Дедлайнды сақтамау баллдардың жоғалуына әкеледі! Әрбір тапсырманың дедлайнды оқу курсының мазмұнын жүзеге асыру күнтізбесінде (кестесінде), сондай-ақ ЖООК-та көрсетілген. Академиялық құндылықтар: - Практикалық / зертханалық сабақтар, СӨЖ өзіндік, шығармашылық сипатта болуы керек. - Бақылаудың барлық кезеңінде плагиатқа, жалған ақпаратқа, көшіруге тыйым салынады. - Мүмкіндігі шектеулі студенттер gulzi200988@mail.ru -мекенжайы бойынша консультациялық көмек ала алады.</p>
Бағалау және аттестаттау саясаты	<p>Критериалды бағалау: дескрипторларға сәйкес оқыту нәтижелерін бағалау (аралық бақылау мен емтихандарда құзыреттіліктің қалыптасуын тексеру). Жиынтық бағалау: аудиториядағы (вебинардағы) жұмыстың белсенділігін бағалау; орындалған тапсырманы бағалау.</p>

Оқыту курсының мазмұнын жүзеге асыру күнтізбесі (кестесі)

Апта / модуль	Тақырып атауы	ОН	ЖИ	Сағат саны	Ең жоғары балл	Білімді бағалау формасы	Сабақты өткізу түрі / платформа
Модуль 1 - Пакеттерді талдау және желілерді ұйымдастыру негіздері							
1	Д 1. Пакеттерді талдау және желілерді ұйымдастыру негіздері	ОН 1	1.1 2.2	1		ӨТС 1	Zoom-да вебинар
	ПС 1. Пакеттік анализаторлардың жұмыс принципі	ОН 1	1.1 1.2	1	2	Талдау	Zoom-да вебинар

	ЗС 1. Виртуалды машиналарға Kali Linux, Eveng орнату және баптау.	ОН 1	2.3	2	8	ТТ 1	Zoom-да вебинар	
Сенбі 23.00 - ӨТС1, ТТ1 тапсыру ДЕДЛАЙНЫ								
2	Д 2. Аралас режимде желіні тыңдау	ОН 1	1.1 2.2	1		ӨТС 2	Zoom-да вебинар	
	ПС 2. Wireshark бағдарламасы арқылы желілік трафикті талдау	ОН 1	1.1 1.2 2.2	1	2	жағдаяттық тапсырма	Zoom да вебинар	
	ЗС 2. Виртуалды машиналарда сынақ зертханасын құру - Kali Linux, Eve-ng баптау.	ОН 1	1.1 1.2 2.3	2	8	ТТ 2	Zoom да вебинар	
	СӨЖ 1. Wireshark пакеттік анализаторымен трафикті сүзу: TCP, UDP, HTTP. Орындалған жұмыс бойынша талдау жасаңыз. СӨЖ 1 орындау бойынша консультация	ОН 1	1.1 1.2 2.2				Zoom да вебинар	
Сенбі 23.00 – ӨТС 2, ТТ2 тапсыру ДЕДЛАЙНЫ								
3	Д 3. Ену тестілеуінің әдіснамасы.	ОН 2	2.1 5.2	1		ӨТС 3	Zoom-да вебинар	
	ПС 3. Сүзілген пакеттерді өңдеу.	ОН 1	1.2 2.2	1	2	Талдау	Zoom да вебинар	
	ЗС 3. Ену тестілерін стандартты өткізу.	ОН 3	3.1 1.2	2	8	ТТ 3	Zoom да вебинар	
Сенбі 23.00 – ӨТС 3, ТТ3 тапсыру ДЕДЛАЙНЫ								
4	Д 4. Алынған нәтижелерді графикалық түрде көрсетуге арналған Wireshark-тың қосымша мүмкіндіктері.	ОН 1	1.1 1.2	1		ӨТС 4	Zoom да вебинар	
	ПС 4. Соңғы нүктелер мен диалогтардың көмегімен ең белсенді желілік түйіндерді анықтау.	ОН 3	3.1 2.2	1	2	жағдаяттық тапсырма	Zoom да вебинар	
	ЗС4. Мақсатты ұйым туралы ақпарат жинау. Eve-ng -де бейнелерді орнату.	ОН 4	4.1 2.2	2	8	ТТ 4	Zoom да вебинар	
	СӨЖ 1. Wireshark пакеттік анализаторымен трафикті сүзу: TCP, UDP, HTTP. Орындалған жұмыс бойынша талдау жасаңыз.	ОН 1 ОН 3	1.1 1.2 2.2		50		Zoom да вебинар	
Сенбі 23.00 – ӨТС4, ТТ4 тапсыру ДЕДЛАЙНЫ								
5	Д 5. Басып шығару және ақпарат жинауға арналған автоматтандырылған құралдар.	ОН 3 ОН 4	3.1 4.2	1		ӨТС 5	Zoom да вебинар	
	ПС 5. Желілік протоколдарды шифрлау.	ОН 2 ОН 4	2.2 4.1	1	2	жағдаяттық тапсырма	Zoom да вебинар	
	ЗС 5. Желілік бағыттау туралы ақпарат алу. Eve-ng баптау.	ОН 1 ОН 4	1.1 4.1	2	8	ТТ 5	Zoom да вебинар	
Сенбі 23.00 – ӨТС5, ТТ5 тапсыру ДЕДЛАЙНЫ								
АБ 1					100			
Модуль II - Автоматтандырылған сканерлеу және ақпарат жинау								
6	Д 6. Kali Linux-та сканерлеу әдістері.	ОН 1 ОН 3	1.1 3.1	1		ӨТС 6	Zoom да вебинар	
	ПС 6. Wireshark-да графиктер тұрғызу.	ОН 1 ОН 2	1.1 2.2	1	2	Талдау	Zoom да вебинар	
	ЗС 6. Kali Linux көмегімен мақсатты машинаны анықтау. Eve-ng өрістету.	ОН 1 ОН 5	1.1 5.1	2	8	ТТ 6	Zoom да вебинар	
Сенбі 23.00 – ӨТС6, ТТ6 тапсыру ДЕДЛАЙНЫ								
7	Д 7. Пакеттерді талдауға арналған командалық жолдың құралдары.	ОН 1 ОН 2	1.1 2.1	1		ТТ 7	Zoom да вебинар	

	ПС 7. Tshark және tcpdump утилиталарының мүмкіндіктері.	ОН 3 ОН 4	3.1 4.1	1	2	зерттеу	Zoom да вебинар
	ЗС 7. Nmap, Netdiscover, Striker, Nipe көмегімен порттарды сканерлеу. Eve-ng баптау.	ОН 3 ОН 5	3.1 5.1	2	8	ТТ 7	Zoom да вебинар
	СӨЖ 2. Kali Linux-мен мобильді енуді тестілеу. Орындалған жұмыс бойынша талдау жасаңыз. СӨЖ 2 орындау бойынша консультация	ОН 4	4.2 2.2				Zoom да вебинар
Сенбі 23.00 – ӨТС7, ТТ7 тапсыру ДЕДЛАЙНЫ							
8	Д 8. Kali Linux-тегі қауіпсіздіктің маңызды кемшіліктерін анықтау және талдау процесі.	ОН 1 ОН 3	1.1 3.1	1		ӨТС 8	Zoom да вебинар
	ПС 8. Wireshark желілік трафик параметрлерін есептеу.	ОН 2 ОН 4	2.2 4.1	1	2	жағдаяттық тапсырма	Zoom да вебинар
	ЗС 8. Осалдықтарды автоматты түрде сканерлеу-Nessus, OpenVAS, Lynis, SPARTA. Eve-ng өрістету.	ОН 2 ОН 4	2.2 4.1	2	8	ТТ 8	Zoom да вебинар
Сенбі 23.00 – ӨТС8, ТТ8 тапсыру ДЕДЛАЙНЫ							
9	Д 9. Kali Linux-тегі әлеуметтік инженердің мақсаттары мен көзқарастарын қалыптастыратын негізгі принциптер.	ОН 2 ОН 3	2.2 3.1	1		ӨТС 9	Zoom да вебинар
	ПС 9. Желілік қабат протоколдары-Wireshark - та желі арқылы деректерді алмасудың негізгі механизмдері.	ОН 1 ОН 4	1.1 4.1	1	2	зерттеу	Zoom да вебинар
	ЗС 9. Kali Linux-та әлеуметтік инженерлік құралдар (әлеуметтік инженерлік құралдар, жиынтық). Eve-ng өрістету.	ОН 2 ОН 4	2.2 4.1	2	8	ТТ 9	Zoom да вебинар
	СӨЖ 2. Kali Linux-мен мобильді енуді тестілеу. Орындалған жұмыс бойынша талдау жасаңыз.	ОН 2 ОН 4	2.2 4.2		50		Zoom да вебинар
Сенбі 23.00 – ӨТС9, ТТ9 тапсыру ДЕДЛАЙНЫ							
10	Д 10. Kali Linux жүйесінде кеңейтілген құралдар жинағы.	ОН 3 ОН 4	3.1 4.1	1		ӨТС 10	Zoom да вебинар
	ПС 10. Splunk-платформаның жалпы сипаттамасы, орнатудың негізгі ерекшеліктері және архитектурасы.	ОН 1 ОН 3	1.2 3.2	1	2	проблемалық жағдайларды талдау	Zoom да вебинар
	ЗС 10. Ашық осалдықтарға және пайдалану кодтарына арналған онлайн-репозиторий. Eve-ng өрістету.	ОН 1 ОН 4	1.2 4.1	2	8	ТТ 10	Zoom да вебинар
Сенбі 23.00 - ӨТС10, ТТ10 тапсыру ДЕДЛАЙНЫ							
MT (Midterm Exam)					100		
Модуль III - Тестілеу құралдары							
11	Д 11. Kali Linux жүйесінде артықшылықтарды арттыру және қол жетімділікті сақтау.	ОН 2 ОН 3	2.2 3.1	1		ӨТС 11	Zoom да вебинар
	ПС 11. Splunk - SPL сұраулары және журналдарды визуализациялау.	ОН 1 ОН 3	1.1 3.2	1	2	зерттеу	Zoom да вебинар
	ЗС 11. Kali Linux-тағы парольдерге дербес шабуыл жасау үшін қолданылатын құралдар. Eve-ng өрістету.	ОН 2 ОН 4	2.1 4.2	2	8	ТТ 11	Zoom да вебинар
Сенбі 23.00 – ӨТС11, ТТ11 тапсыру ДЕДЛАЙНЫ							
12	Д 12. Kali Linux-та веб-қосымшаларды тестілеу.	ОН 3 ОН 5	3.1 5.1	1		ӨТС 12	Zoom да вебинар
	ПС 12. Splunk - статистикалық сұраулар мен визуализация.	ОН 1 ОН 3	1.2 3.1	1	2	проблемалық жағдайларды талдау	Zoom да вебинар
	ЗС 12. Веб-қосымшалардағы осалдықтарды анықтауға арналған құралдар: OWASP ZAP, nikto, sqlmap және Burp Suite. Eve-ng өрістету.	ОН 2 ОН 4	2.1 4.1	2	8	ТТ 12	Zoom да вебинар

	СӨЖ 3. EVE-NG платформасын қолдана отырып, желілік шабуылдарды модельдеу. Орындалған жұмыс бойынша талдау жасаңыз. СӨЖ 3 орындау бойынша консультация	ОН 1 ОН 3	1.1 3.2				Zoom да вебинар
Сенбі 23.00 - ӨТС12, ТТ12 тапсыру ДЕДЛАЙНЫ							
13	Д 13. Kali Linux сымсыз желілерге енуді тестілеу.	ОН 1 ОН 4	1.1 4.1	1		ӨТС 13	Zoom да вебинар
	ПС 13. SPLUNK - есеп беру, ескерту және жауап беру схемаларын құру.	ОН 2 ОН 4	2.2 4.1	1	2	жағдаяттық тапсырма	Zoom да вебинар
	ЗС 13. Kali Linux жүйесінде сымсыз желілерді анықтау. Eve-ng өрістету.	ОН 2 ОН 4	2.2 4.1	2	8	ТТ 13	Zoom да вебинар
Сенбі 23.00 - ӨТС13, ТТ13 тапсыру ДЕДЛАЙНЫ							
14	Д 14. Kali Linux жүйесінде сымсыз желіні тестілеу құралдары.	ОН 1 ОН 4	1.1 4.1	1		ӨТС 14	Zoom да вебинар
	ПС 14. Splunk - деректер көздері, деректерді индексстеу және индекс ұғымы.	ОН 2 ОН 3	2.1 3.2	1	2	проблемалық жағдайларды талдау	Zoom да вебинар
	ЗС 14. Kali Linux-тегі сымсыз трафикті талдау. Eve-ng өрістету.	ОН 3	3.1 3.2	2	8	ТТ 14	Zoom да вебинар
	СӨЖ 3. EVE-NG платформасын қолдана отырып, желілік шабуылдарды модельдеу. Орындалған жұмыс бойынша талдау жасаңыз.	ОН 1 ОН 3	1.1 3.2		50		Zoom да вебинар
Сенбі 23.00 - ӨТС14, ТТ14 тапсыру ДЕДЛАЙНЫ							
15	Д 15. Ену тестілеуі туралы есептер жасауға арналған құралдар.	ОН 1 ОН 5	1.1 5.2	1		ӨТС 15	Zoom да вебинар
	ПС 15. Splunk қосымшалары мен қондырмалары (Apps және Add-ons).	ОН 1 ОН 5	1.1 5.1	1	2	проблемалық жағдайларды талдау	Zoom да вебинар
	ЗС 15. Kali Linux, Eve-ng есептер түрлері.	ОН 1 ОН 5	1.1 5.2	2	8	ТТ 15	Zoom да вебинар
Сенбі 23.00 - ӨТС15, ТТ15 тапсыру ДЕДЛАЙНЫ							
	АБ2				100		

Қысқартулар: ӨТС – өзін-өзі тексеру үшін сұрақтар; ТТ – типтік тапсырмалар; АБ – аралық бақылау.

Декан

Әдістемелік бюро төрайымы

Кафедра меңгерушісі

Аға оқытушы

Урмашев Б.А.

Ғұсманова Ф.Р.

Мүсіралиева Ш.Ж.

Ордабаева Г.К.