Әл-Фараби атындағы Қазақ ұлттық университеті
Ақпараттық технологиялар факультеті

СИЛЛАБУС
2020-2021 оқу жылының күзгі 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 3301	Желілік қауіпсіздік 1	98	15	15	15	5	6

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	Емтихан
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)**
Студенттерде қазіргі заманғы бағдарламалық-аппараттық құралдарды қолдана отырып компьютерлік желілерді қорғау бойынша білім мен дағдыларды қалыптастыру	**ОН 1** (когнитивті) - Қорғалған компьютерлік жүйелер қауіпсіздігі әкімшісінің функцияларын пайдалана білу;	1.1. Шабуылдардың нақты мысалдарын анықтау және жіктеу; 1.2. Осалдық, қауіп және шабуыл жағдайларын талдау;
	ОН 2 (функционалды) - Желілік бағдарламалық - аппараттық құралдар қорғаныш тетіктерін баптауды игеру;	2.1. Компьютерлік желілер үшін ақпаратты қорғаудың түрлі әдістері мен құралдарын тиімді пайдалану үшін тәжірибе жасау; 2.2. Желілердегі осалдықтың себептерін түсіндіру;
	ОН 3 (функционалды) - Қорғалған компьютерлік желілер жасау мақсатында іске асырылған бағдарламалық-аппараттық кешендерде қорғау механизмдерін талдау және болжауды игеру;	3.1. Компьютерлік желілердің қауіпсіздігіне қауіп-қатер мониторингін жүргізуді әзірлеу; 3.2. Желілік қауіпсіздікті қамтамасыз ету қажеттілігін анықтайтын факторларды талқылау;
	ОН 4 (жүйелік) - Желіаралық экрандарды пайдалана отырып компьютерлік желі сегменттерін қорғауды ұйымдастыру;	4.1. Қауіпсіздікті қамтамасыз ету хаттамаларын талдау әдістерін ұйымдастыру; 4.2. Қауіпсіз компьютерлік желілерді құру мақсатында бағдарламалық-аппараттық кешендерде қолданылатын қорғау механизмдеріне баға беру;
	ОН 5 (жүйелік) - Компьютерлік желі тораптарында анықталған бағдарламалық қамтамасыз ету осалдықтары әдістері және құралдарын зерттеу.	5.1. Компьютерлік желілерді жобалау және басқару әдістемелерін таңдау; 5.2. Компьютерлік желінің қауіпсіздік саясатын іске асыру жолдарын салыстыру;

Пререквизиттер	Ақпараттану, Алгоритімдік тілдерде программалау
Постреквизиттер	Жүйелік программалық қамтамасыздандыру, Таратылған жүйелер технологиясы, Жасанды интеллект жүйелері
Әдебиет және ресурстар	**Әдебиеттер**: *Негізгі*: 1. Лапонина О.Р. Основы сетевой безопасности. Часть 1. Межсетевые экраны: Учебное пособие / О.Р. Лапонина — М.: Национальный Открытый Университет «ИНТУИТ», 2014. — 378 с., ил., табл.— (Серия «Основы информационных технологий») 2. Бобровский С. М. Лабораторный практикум по дисциплине «Защита информационных процессов в компьютерных системах и телекоммуникационных сетях» / сост. С. М. Бобровский. – Тольятти : Изд-во ПВГУС, 2016. – 84 с. *Қосымша* 1. Uenstrom M. Securing networks Cisco. – M.: Williams, 2015. – 698 p. 2. D. Chapman, Fox E. Firewalls Cisco Secure PIX. – M.: Williams, 2013. – 548 p. 3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. - М.: Форум-Инфра-М, 2013. – 416 с. 4. Бирюков А.А. Информационная безопасность. Защита и нападение. – М.: ДМК-Пресс, 2012. – 474 с. 5. Платонов В.В. Программно-аппаратные средства защиты информации. – М.: Academy, 2013. – 336 с. 6. Bragg R. Rhodes Owsley M. Strassberg KE Network Security. Complete Guide – M: Economy, 2016. – 312 p. *Интернет-ресурстар*: 1. https://www.virtualbox.org 2. https://linux.org 3. https://ubuntu.ru

Университеттік моральдық-этикалық құндылықтар шеңберіндегі курстың академиялық саясаты	**Академиялық тәртіп ережелері:** Барлық білім алушылар ЖООК-қа тіркелу қажет. Онлайн курс модульдерін өту мерзімі пәнді оқыту кестесіне сәйкес мүлтіксіз сақталуы тиіс. **НАЗАР АУДАРЫҢЫЗ!** Дедлайндарды сақтамау баллдардың жоғалуына әкеледі! Әрбір тапсырманың дедлайны 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.
Бағалау және аттестаттау саясаты	**Критериалды бағалау:** дескрипторларға сәйкес оқыту нәтижелерін бағалау (аралық бақылау мен емтихандарда құзыреттіліктің қалыптасуын тексеру). **Жиынтық бағалау:** аудиториядағы (вебинардағы) жұмыстың белсенділігін бағалау; орындалған тапсырманы бағалау.

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. Корпоративтік желінің ақпараттық инфрақұрылымының деңгейлері							
1	**Д 1.** Компьютерлік желілер шабуылдары ұғымы және жіктелуі.	ОН 1	1.1	1		ӨТС 1	Zoom- да вебинар
	ПС 1. Қауіпсіздік жүйесіндегі осалдықты анықтау.	ОН 2	1.1 3.1	1	2	ТТ1	Zoom- да вебинар
	ЗС 1. Linux (Ubuntu) операциялық жүйесін орнату және оның пайдаланушылық интерфейсімен танысу.	ОН 3	1.1	2	8	ӨТС 1	Zoom- да вебинар

	Сенбі 23.00 - ӨТС1, ТТ1 тапсыру ДЕДЛАЙНЫ						
2	**Д 2.** Желілік шабуылдардың негізгі түрлері. Шабуылдарды жүзеге асыру құралдары.	ОН 1	1.1 2.2	1		ӨТС 2	Zoom- да вебинар
	ПС 2. Желілік порттарды сканерлеу-Nmap қосымшасы	ОН 3	4.1 5.2	1	2	Талдау	Zoom да вебинар
	ЗС 2. Linux жүйесіндегі жүйелік монитор (Тапсырма менеджері)	ОН 5	5.2 1.2	2	8	ӨТС 2	Zoom да вебинар
	Сенбі 23.00 – ӨТС 2 тапсыру ДЕДЛАЙНЫ						
3	**Д 3.** Осал желілік хаттамаларға негізделген типтік шабуылдар механизмдері.	ОН 2	2.2 5.2	1		ӨТС 3	Zoom- да вебинар
	ПС 3. OpenVAS – осалдықты анықтау қосымшасы.	ОН 3	3.2 1.1	1	2	Талдау	Zoom да вебинар
	ЗС 3. Жүктеуші флэш-жинақтауышты құру. Ubuntu Linux файлдық жүйелері.	ОН 5	5.1 1.1	2	8	ӨТС 3	Zoom да вебинар
3	**СӨЖ 1.** Желінің осалдықтарын іздеу және пайдалану қосымшаларына талдау.	ОН 1	1.1 5.2		25		Zoom да жазбаша
	Сенбі 23.00 – ӨТС 3 тапсыру ДЕДЛАЙНЫ						
4	**Д 4.** Желілік қызметтерге шабуыл.	ОН 2	2.2 5.2	1		ӨТС 4	Zoom да вебинар
	ПС 4. Nexpose Community Edition – осалдықты анықтау қосымшасы.	ОН 4	4.1 1.2	1	2	Талдау	Zoom да вебинар
	ЗС4. Файлдық жүйемен жұмыс: file, mv, cp, rmdir, ps, kill 9, find, sort, clear.	ОН 5	5.1 1.2	2	8	ӨТС 4	Zoom да вебинар
	СӨЖ 2. Терминал терезелері және консольмен жұмыс.	ОН 5	5.2 1.2		25		Zoom да жазбаша
	Сенбі 23.00 – ӨТС4 тапсыру ДЕДЛАЙНЫ						
5	**Д 5.** Аралық тораптар мен аумақтарды пайдалана отырып жүргізілетін шабуылдар.	ОН 1	1.1 5.1	1		ӨТС 5	Zoom да вебинар
	ПС 5. Metasploit Framework бағдарламасын орнату және оның пайдаланушылық интерфейсімен танысу.	ОН 2	3.1 2.2	1	2	Талдау	Zoom да вебинар
	ЗС 5. Файлдық жүйемен жұмыс: cmp, df, apt get install, remove, update, upgrade, chmod.	ОН 3	3.1 5.2	2	8	ӨТС 5	Zoom да вебинар
	Сенбі 23.00 – ӨТС5 тапсыру ДЕДЛАЙНЫ						
	АБ 1				**100**		
Модуль II. Арналық деңгейде желілерді сегменттеу							
6	**Д 6**. Пакеттер фильтрациясы. Фильтрация ережелері және критерийлері.	ОН 3	3.1 1.2	1		ӨТС 6	Zoom да вебинар
	ПС 6. Қауіпсіздікті тестілеу әдістемесі.	ОН 4	4.1 2.2	1	2	Талдау	Zoom да вебинар

	ЗС 6. Linux терминалы: gksu, pstree, top, screenfetch, қатты дискіні жазып, жүктеу бөлімін тазалау.	ОН 5	5.2 1.2	2	8	ӨТС 6	Zoom да вебинар
	Сенбі 23.00 – ӨТС6 тапсыру ДЕДЛАЙНЫ						
7	**Д 7**. Демилитаризациялық аймақ түсінігі.	ОН 2	2.2 5.2	1		ӨТС 7	Zoom да вебинар
	ПС 7. Metasploit Framework осалдықты анықтау.	ОН 3	3.1 1.2	1	2	Талдау	Zoom да вебинар
	ЗС 7. Серверге физикалық қол жеткізу кезінде root паролін қалпына келтіру мүмкіндіктері	ОН 4	4.2 2.2	2	8	ӨТС 7	Zoom да вебинар
	Сенбі 23.00 – ӨТС7 тапсыру ДЕДЛАЙНЫ						
8	**Д 8**. Шабуылдаушының назарын аудару үшін тораптарды ұйымдастыру.	ОН 2	2.1 5.1	1		ӨТС 8	Zoom да вебинар
	ПС 8. Желілік сервистердегі осалдықтарды пайдалану.	ОН 1	1.1 4.2	1	2	Талдау	Zoom да вебинар
	ЗС 8. Аутентификация қосылатын модульдері (PAM)	ОН 3	3.2 1.1	2	8	ӨТС 8	Zoom да вебинар
	СӨЖ 3. ARP адресін шешу протоколының қауіпсіздік мәселелері.	ОН 2	2.1 4.2		25		Zoom да жазбаша
	Сенбі 23.00 – ӨТС8 тапсыру ДЕДЛАЙНЫ						
9	**Д 9.** 802.1 x стандартының талаптарын қанағаттандыратын желілік инфрақұрылымды құру кезеңдері.	ОН 2	2.1 4.2	1		ӨТС 9	Zoom да вебинар
	ПС 9. Әр түрлі трафикті сүзу мүмкіндіктері.	ОН 3	3.1 2.2	1	2	Талдау	Zoom да вебинар
	ЗС 9. SELinux саясатының жұмыс механизмі. Қол жеткізу ережелерін сипаттау тілі.	ОН 5	5.1 4.2	2	8	ӨТС 9	Zoom да вебинар
	СӨЖ 4. ARP протоколы, Cain утилитасы арқылы желілік анализаторларды анықтау.	ОН 4	4.2 1.2		25		Zoom да жазбаша
	Сенбі 23.00 – ӨТС9 тапсыру ДЕДЛАЙНЫ						
10	**Д 10.** Желіаралық экрандар және олардың түрлері.	ОН 4	4.1 1.2	1		ӨТС 10	Zoom да вебинар
	ПС 10. Address Spoofing шабуылынан қорғау.	ОН 3	3.2 1.1	1	2	Талдау	Zoom да вебинар
	ЗС 10. Оқиғаларды тіркеу жүйесін орнату.	ОН 2	2.1 5.2	2	8	ӨТС 10	Zoom да вебинар
	Сенбі 23.00 - ӨТС10 тапсыру ДЕДЛАЙНЫ						
	МТ (Midterm Exam)				**100**		
Модуль ІІІ. Енуді анықтау және алдын алу жүйелері							
11	**Д 11.** VPN арқылы шешілетін тапсырмалар. Қорғалған арналар деңгейлері.	ОН 5	5.1 3.2	1		ӨТС 11	Zoom да вебинар
	ПС 11. OSI моделінің желілік деңгейінің қауіпсіздігі.	ОН 3	3.2 1.2	1	2	Талдау	Zoom да вебинар

	ЗС 11. Syslog негізінде орталықтандырылған қауіпсіздік оқиғаларын басқару жүйесін құру.	ОН 2	2.1 1.2	2	8	ӨТС 11	Zoom да вебинар
	Сенбі 23.00 – ӨТС11 тапсыру ДЕДЛАЙНЫ						
12	**Д 12**. Checkpoint NGX брандмауэрінің негізгі мүмкіндіктерін зерттеу.	ОН 4	4.2 2.1	1		ӨТС 12	Zoom да вебинар
	ПС 12. Address Spoofing шабуылынан қорғау.	ОН 3	3.1 1.1	1	2	Талдау	Zoom да вебинар
	ЗС 12. Linux ОЖ негізіндегі IPTABLES пакеттік сүзгісі.	ОН 4	4.1 1.2	2	8	ӨТС 12	Zoom да вебинар
	СӨЖ 5. IPv6 нұсқасының қауіпсіздік мәселелері.	ОН 3	3.1 5.2		25		Zoom да жазбаша
	Сенбі 23.00 - ӨТС12 тапсыру ДЕДЛАЙНЫ						
13	**Д 13**. Брандмауэр ішкі саясаты.	ОН 4	4.2 1.2	1		ӨТС 13	Zoom да вебинар
	ПС 13. ICMP хаттамасын қолдана отырып жасалған шабуылдар.	ОН 2	2.1 1.2	1	2	Талдау	Zoom да вебинар
	ЗС 13. SSH хаттамасы. Қашықтан басқару құралын қорғау.	ОН 2	2.2 1.1	2	8	ӨТС 13	Zoom да вебинар
	Сенбі 23.00 - ӨТС13 тапсыру ДЕДЛАЙНЫ						
14	**Д 14**. NAT мүмкіндіктері бар желіаралық экрандар.	ОН 4	4.2 1.1	1		ӨТС 14	Zoom да вебинар
	ПС 14. VPN технологияларын пайдалану схемалары. IPsec туралы ақпарат.	ОН 4	4.1 2.1	1	2	Талдау	Zoom да вебинар
	ЗС 14. SSH қауіпсіздігін арттыру. Әр түрлі желілік ортадан қосылу.	ОН 3	3.1 2.1	2	8	ӨТС 14	Zoom да вебинар
	СӨЖ 6. Алдын алу механизмі ретінде корпоративтік желінің қауіпсіздігін талдау.	ОН 5	5.2 2.2		25		Zoom да жазбаша
	Сенбі 23.00 - ӨТС14 тапсыру ДЕДЛАЙНЫ						
15	**Д 15**. Желіаралық экрандарды пайдалану кезіндегі желі топологиясы	ОН 4	4.1 5.1	1		ӨТС 15	Zoom да вебинар
	ПС 15. Желілік қауіпсіздік сканерлерінің мүмкіндіктері мен пайдалану жағдайлары. Internet Scanner бағдарламасымен жұмыс.	ОН 5	4.2 3.2		2	Талдау	Zoom да вебинар
	ЗС 15. Apache+MySQL+PHP серверінің мысалында UNIX жүйелеріндегі қолданбалы қызметтерді қорғау ерекшеліктері.	ОН 5	4.1 5.2	2	8	ӨТС 15	Zoom да вебинар
	Сенбі 23.00 - ӨТС15 тапсыру ДЕДЛАЙНЫ						
	АБ2				**100**		

Әдістемелік бюро төрайымы Ғұсманова Ф.Р.

Кафедра меңгерушісі Мүсіралиева Ш.Ж.

Аға оқытушы Ордабаева Г.К.