СӘТБАЕВ УНИВЕРСИТЕТІ SATBAYEV UNIVERSITY

Автоматика және ақпараттық технологиялар институты

Киберқауіпсіздік кафедрасы

БЕКІТЕМІН
АжАТ институтының директоры
_____ Дайнеко Е.А.
«24» 06 2026 ж.

СИЛЛАБУС

SEC1811 Ақпаратты криптографиялық қорғау негіздері

6В06301 Ақпараттық қауіпсіздік

Пән циклы БП, 5 (1/1/1/2) кредит

3 курс, **5** семестр

2026- 2027 оқу жылы

Алматы 2026

1. Оқытушылар туралы ақпарат

1.1 Лекторлар:

1. Алимсеитова Жулдыз Кенесхановна, профессор,
кеңсе: кабинет 325ГУК
Офис-сағаты: _____
e-mail: zh.alimseitova@satbayev.university.

2. Ахмедиярова Айнур Танатаровна, профессор
кеңсе: кабинет 325ГУК
Офис-сағаты: _____
e-mail: a.akhmedyarova@satbayev.university

1.2 Практикалық/зертханалық жұмысты жүргізетін оқытушылар

1. Ахмеди Гулдана, ассистент
кеңсе: кабинет 325ГУК
Офис-сағаты:_____
e-mail: g.akhmedi@satbayev.university

2. Ержан Әсел Ержанқызы, преподаватель
кеңсе: кабинет 325ГУК
Офис-сағаты: _____
a.yerzhan@satbayev.university

3. Омар Айым, преподаватель
кеңсе: кабинет 325ГУК
Офис-сағаты: _____
a.omar@satbayev.university

***Оқу түрі - күндізгі**

2. Пререквизиттер мен постреквизиттер

Пререквизиттер	SEC114 Мамандыққа кіріспе
Постреквизиттер	SEC190 Ақпараттық қауіпсіздіктің криптографиялық жүйелері

3. Курстың мақсаты мен міндеттері

Мақсаты: ақпаратты рұқсатсыз қатынас құрудан, өзгертуден, жоюдан тиімді қорғау үшін криптографиялық қорғау негіздерін игеру және практикалық түрде қолдану.

Курсты оқу келесі мақсаттарға қол жеткізуге үлес қосады:

- ТДМ 4 «Сапалы білім беру» - цифрлық сауаттылықты, криптографиялық жүйелерді қолдану және құру дағдыларын, сыни ойлауды және өз бетінше оқытуды дамыту;
- ТДМ 8 «Лайықты жұмыс және экономикалық өсу» – криптографиялық жүйелерді құру, қолдану және жобалауды қамтамасыз ету нарығында сұранысқа ие құзыреттерді қалыптастыру;
- ТДМ 9 «Индустрияландыру, инновациялар және инфрақұрылым» - цифрлық инновациялар, ұйымның инфрақұрылымын қорғау үшін ақпаратты криптографиялық қорғау саласындағы құзыреттерді дамыту;
- ТМД 10 «Теңсіздікті азайту» - мүмкіндігі шектеулі жандарға қол жетімді интерфейстерді жобалау;

- ТДМ 16 «Бейбітшілік, сот төрелігі және тиімді институттар» - криптографиялық қорғау бағытындағы этиканы, стандарттарды, заңдарды зерделеу, цифрлық ортада жауапты мінез-құлықты қалыптастыру.

Міндеті:

- криптографияның негізгі түсініктемелері мен анықтамаларын, негізгі ережелерін білу;
- криптографиялық жүйелерінің жіктеліуін, криптографияның қолдану аясын білу;
- криптографиялық жүйелерді ақпаратты қорғау үшін, деректердің тұтастығын қамтамасыз ету үшін, шынайлығын дәлелдеу үшін қолдану.

4. Курстың сипаттамасы:

Курс «6В06301 – «Ақпараттық қауіпсіздік» білім беру бағдарламасы бойынша білім алушыларға арналған.

Пән аясында студенттер ақпаратты криптографиялық қорғаудың негіздерін, қолдану аясын, мақсатын оқиды. Криптографияның негізгі түсініктерін, мақсатын, қолдану аясын, математикалық негіздерін, негізгі принциптерін, шифрлар жіктелуін, классикалық шифрларды, оларды криптоталдауды, құрамдас шифрларды, асимметриялық шифрларды, кілттерді тарату әдістерін практикалық қолдануды меңгереді.

5. Оқу нәтижелері

Курсты аяқтағаннан кейін білім алушы:

Білуі керек:

- криптографияның негізгі түсініктемелері мен анықтамаларын;
- криптографиялық қорғаудың мақсатын, принциптерін;
- шифрларды құрамдастыру әдістерін;
- классикалық шифрлау алгоритмдерін, олардың кемшіліктері мен артықшылықтарын;
- криптографияның математикалық негіздерін;
- криптографияның симметриялық және асимметриялық әдістерін;
- блокты және ағынды шифрлардың жұмыс істеу принциптерін;
- асимметриялық шифрлардың жұмыс істеу принциптерін;
- шифрлардың жұмыс істеу принциптерін

Істей алуы керек:

- криптографиялық қорғау жүйелерін файлдарды қорғау үшін қолдану;
- криптографиялық әдістерді қолдану арқылы ақпараттың тұтастығын қамтамасыз ету;
- криптографиялық жүйелердің тиімділігін арттыру үшін кілттерді дұрыс генерациялау және тарату;
- криптографиялық хаттамаларды қолдану.

Дағдыларды меңгеру:

- криптографиялық жүйелерді ақпараттың кез келген түрін қорғау;
- криптографиялық жүйелердің тиімділігін және сенімділігін бағалау;
- ақпаратты криптографиялық қорғау бағдарламалары мен құралдарын қолдану;
- криптографиялық жүйелерді жобалау.

6. Күнтізбелік-тақырыптық жоспары

Апта	Дәріс тақырыбы	Практикалық жұмыстар тақырыбы	Зертханалық жұмыстар тақырыбы	СӨЖ, СОӨЖ	Әдебиетке сілтеме	Тапсыру уақыты
1	Кіріспе. Негізгі түсініктемелер мен анықтамалар. Криптография тарихы. Шифрлардың формалды үлгілері.	П№1 Криптографиялық жүйенің жалпылама сұлбасы	З№1 Аффинды шифр, Цезарь шифры, қарапайым ауыстыру шифры		[1] 11-21 б., [4] 285-294 б., [6]	З№1
2	Әртүрлі признактар бойынша шифрларды жіктеу. Беріктілік, қорғалғандық, имитобериктілік, аутентификациялық.	П№2 Криптографиялық талдау.	З№2 Транспозиция шифры, Бағанды ауыстыру шифры. Екі рет ауыстыру шифры.		[2] 125-136 б., [3] 196-200 б., [5] 44-54 б., [6]	З№2
3	Ауыстыру шифрларының математикасы. Ағынды, блокты, көпалфавитты, дискті	П№3 Ауыстыру шифрларын криптоталдау әдістері	З№3 Блокты ауыстыру шифрлары	Аффинды шифрын криптоталдау	[1] 45-58 б., [2] 136-140 б., [5] 55-64 б., [6]	З№3, СӨЖ
4	Гаммалау шифрларының математикасы.	П№4 Гаммалау шифрлары	З№4 Виженер, Хилл шифрлары		[1] 89-101 б., [2] 185-196 б., [3] 29, 95-115 б., [6]	З№4
5	Кодтау. Композициялық шифрлар.	П№5 Кодтау әдістері	З№5 Шифрлардың композициялары	Виженер шифрын криптоталдау	[1] 116-204 б., [2] 125-127 б., [3] 29, 95-115 б., [6]	П№5, СОӨЖ
6	Математикалық негіздер: модульдік арифметика, Евклид және	П№6 Сандар теориясының негіздері. Евклид алгоритмі.	З№6 Кеңейтілген Евклид алгоритмі		[1] 207-264 б., [2] 115-118, 201-202 б., [5] 143-	П№6

Апта	Дәріс тақырыбы	Практикалық жұмыстар тақырыбы	Зертханалық жұмыстар тақырыбы	СӨЖ, СОӨЖ	Әдебиетке сілтеме	Тапсыру уақыты
	кеңейтілген Евклид алгоритмі				150 б., [6]	
7	Модульдік дәреже. Эйлер Теоремасы.	ПЖ№7 Эйлер теоремасы	ЗЖ№7 Модульдік дәреже бойынша есептер		[1] 307-389 б., [2] 118-122, 163-166 б., [5] 198-262 б., [6]	ЗЖ№7
	Қытай қалдықтары теоремасы.	ПЖ№8 Қытай қалдықтары теоремасы бойынша есептер	ЗЖ№8 Плейфер шифры және оны криптоталдау		[1] 397-412 б., [2] 149-167 б., [4] 385-419 б., [6]	ЗЖ№8
	Бірінші аралық аттестация					8 апта
9	Ферма теоремасы.	ПЖ№9 Ферма теоремасы бойынша есептер	ЗЖ№9 Рюкзак жинау шифры	Транспозиция шифрын криптоталдау	[1] 414-432 б., [3] 245-256 б., [6]	ЗЖ№9 СОӨЖ
10	Құрамдас шифрлар. Шашырату және араластыру. Раундтар.	ПЖ№10 Шашырату және араластыру бойынша есептер.	ЗЖ№10 Шашырату және араластыру.		[1] 433-458 б., [4] 419-433 б., [6]	ПЖ№10
11	Симметриялық криптожүйелер және құру принципі. Фейстель желісі.	ПЖ№11 Фейстель желісі.	ЗЖ№11 Екі бұтақты Фейстель желісі		[1] 459-498 б., [2] 170-234 б., [6]	ЗЖ№11
12	Ашық кілтті криптожүйелер. Асимметриялық криптографиялық алгоритмдер.	ПЖ№12 RSA шифрының математикасы	ЗЖ№12 RSA шифры	Туған күн парадоксы шабуылы	[1] 459-498 б., [2] 170-234 б., [6]	ЗЖ№12, СӨЖ
13	Кілттерді бөлу хаттамалары. Ашық кілтті басқару	ПЖ№13 Ашық кілтті басқару әдістері	ЗЖ№13 Кілттерді бөлу хаттамасы		[1] 459-498 б., [2] 170-234 б., [6]	ПЖ№13, ЗЖ№13
14	Энтропия және тілдің артықтығы. Бірлік аралық.	ПЖ№14 Энтропия және тілдің артықтығы бойынша есептер	ЗЖ№14 Бірлік аралық		[1] 459-498 б., [2] 170-234 б., [6]	ЗЖ№14
15	Шифрлардың беріктілігі.	ПЖ№15 Шифрлардың теориялық	ЗЖ№15 Шифрлардың практикалықбе		[2] 235-246 б., [6]	ЗЖ№15

Апта	Дәріс тақырыбы	Практикалық жұмыстар тақырыбы	Зертханалық жұмыстар тақырыбы	СӨЖ, СОӨЖ	Әдебиетке сілтеме	Тапсыру уақыты
		беріктілігін бағалау	ріктілігін бағалау			
	Екінші аралық аттестация					15 апта
	Қорытынды емтихан жазбаша					Кесте бойынша

7. Әдебиет

Негізгі әдебиет	Қосымша әдебиет
1. Ахметов Б.С., Корченко А.Г., Сиденко В.П., Дрейс Ю.А., Алимсеитова Ж.К. Қолданбалы криптология: шифрлау әдістері. Оқулық. Алматы: ҚазҰТЗУ, 2016 - 500 б.	7. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. М.: Аст, Астрель, 2006. 447 с.
2. Ахметов Б.С., Кузнецов А.А., Краснобаев В.А., Алимсеитова Ж.К., Кузнецова Т.Ю. Криптография негіздері: сандар теориясының, топтардың, өрістердің, сақиналардың элементтері. Оқу құралы. - Алматы: АЭжБУ, 2020 – 320б.	8. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003. 806 с.
3. Васильева И. Н. Криптографические методы защиты информации. М.: Юрайт. 2024. 350 с.	9. Мао В. Современная криптография. Теория и практика. М.: Вильямс, 2005. 763 с.
4. Лось А. Б., Нестеренко А. Ю., Рожков М. И. Криптографические методы защиты информации для изучающих компьютерную безопасность. М.: Юрайт. 2024. 474 с.	
5. Омассон Жан-Филипп. О криптографии всерьез. Практическое введение в современное шифрование. М.: ДМК Пресс. 2021. 328 с.	
6. Рацеев С. М. Математические методы защиты информации и их основы. Сборник задач. М.: Лань. 2023. 140 с.	

8. Құзыреттілік шеңбері

Оқыту дескрипторлары	Құзыреттілік				
	Ғылыми-жаратылыстану және теориялық-дүниетанымдық	Әлеуметтік-жеке және азаматтық	Жалпы инженерлік, кәсіби	Мәдениетаралық және коммуникативтік	Арнайы мамандандырылған
Білім және түсінік	Зерттеудің негізгі түрлерін түсіну	Зерттеулер мен эксперименттердің әлеуметтік	Инженерлік зерттеу әдістерін білу	Зерттеу кезінде мәдениетаралық және коммуника-	Пайдалану, жобалау, әзірлеу және тестілеуді

		және этикалық аспектілерін түсіну		тивті білімге ие болу	білу және түсіну
Білім мен түсінікті қолдану	Ғылыми зерттеу әдістерін қолдану	Топтық жұмыс дағдыларын қолдану және әртүрлі пікірлерді құрметтеу	Зерттеу жұмысында инженерлік әдістерді әзірлеу және қолдану	Зерттеулерді заманауи инновациялар мен бағдарламаларға бейімдеу	Кәсіби қызметте білім мен түсініктерді қолдану
Пікір білдіру және әрекеттерді талдау	Зерттеулердің ғылым мен қоғамның дамуына әсерін талдау	Технологияның әлеуметтік әсерін талдау және бағалау	Инженерлік шешімдердің тиімділігін талдау	Әр түрлі әріптестердің зерттеу тәсілдерін салыстыру	Зерттеулердегі осалдықтар мен қателіктерді анықтау
Коммуникативтік және шығармашылық қабілеттер	Ғылыми идеяларды қолжетімді түрде ұсыну	Командада жұмыс істеу және әріптестердің пікірін құрметтеу	Визуалды және инженерлік коммуникация құралдарын пайдалану	Мәдениетаралық коммуникацияны орнату	Кәсіби қызметте шығармашылықты көрсету
Өздігінен білім алу және цифрлық дағдылар	Үздіксіз оқу қабілетін дамыту	Өзінің дамуы мен академиялық адалдығы үшін жауапкершілікті қабылдау	Цифрлық инженерлік құралдарды қолдану және дамыту	Өзара әрекеттесу және оқыту үшін цифрлық платформаларды пайдалану	Кәсіби қызмет үшін заманауи әдістер мен цифрлық дағдыларды игеру

9. Қажетті жұмыстарды тапсыру кестесі

№ р/с	Бақылау түрі	Аптаның макс. баллы	Апта															
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Макс балл қорытындысы
1	Дәріс сабақтарындағы белсенділік	0																60
2	Білім алушының оқытушымен өзіндік жұмысы (СОӨЖ)	2,5					2,5				2,5							
3	Білім алушының өзіндік жұмысы (СӨЖ)	2,5			2,5									2,5				
4	Тәжірибелік тапсырмаларды орындау	2,5					2,5	2,5				2,5			2,5			
5	Зертханалық	2,5	2,5	2,5	2,5	2,5			2,5	2,	2,5		2,5	2,5	2,5	2,5	2,5	

	тапсырмаларды орындау									5								
6	1-ші аралық бақылау	5								5								
7	2-ші аралық бақылау	5															5	
8	Қорытынды емтихан*																	40
	Барлығы																	100

10. Бағалау рейтингі және критерийлер бойынша бағалаудың мүмкін болатын соңғы нұсқалары

Әріптік жүйе бойынша бағалау	Ұпайлардың сандық баламасы	Пайыздық көрсеткіш	Критерийлері	Дәстүрлі жүйе бойынша бағалау
A	4	95-100	Оқытылатын курс көлемінен асатын білімнің ең жоғарғы стандарттарын көрсетеді	«Өте жақсы»
A-	3,67	90-94	Білімнің ең жоғары стандарттарына сәйкес келеді	
B+	3,33	85-89	Өте жақсы және білімнің жоғары стандарттарына сәйкес келеді	«Жақсы»
B	3	80-84	Жақсы және білімнің жоғары стандарттарына сәйкес келеді	
B-	2,67	75-79	Жоғары стандарттарға жақын жеткілікті білім	
C+	2,33	70-74	Жалпы стандарттарға сәйкес келетін жеткілікті білім	
C	2	65-69	Жалпы білім стандарттарының көбіне сәйкес келеді және қанағаттандырарлық білім	«Қанағаттанарлық»
C-	1,67	60-64	Қанағаттандырарлық, бірақ кейбір білім бойынша стандарттарға сәйкес келмейді	
D+	1,33	55-59	Минималды қанағаттандырады, бірақ кең ауқымды білім стандарттарына сәйкес келмейді	
D	1	50-54	Стандарттарға сәйкес келуі күмәнді минималды қанағаттандырарлық өту балы	
FX	0,5	25-49	Уақытша бағалау: қанағаттанарлықсыз төменгі көрсеткіш, емтиханды қайта тапсыруды қажет етеді	«Қанағаттанарлықсыз»
F	0	0-24	Пәнді игеруге тырыспады. Студент емтиханнан айла арқылы баға алмақ болған кезде де қойылады	

11. Бағалау критерийлері

Тесттен басқа әр жұмыс 4 критерий бойынша бағаланады:

– ұқыптылық пен дәлдік (А)– 30% (жұмыс қаншалықты ұқыпты және дәл есептелген);

– шығармашылық және креативтілік (Т) - 30% (жұмыс қалай және қандай үлгіде ұсынылған);

– толықтығы мен жетілуі (З) - 40% (жұмыс қаншалықты терең, қисынды және құрылымдық түрде шешілді);

– ерекшелік (О) – арнайы 1.0; 0.5 немесе 0 коэффициенті қолданылады.

Критерийлері	Өте жақсы (0.9-1.0)	Жақсы (0.7-0.9)	Қанағаттанарлық (0.4-0.7)	Қанағаттанарлықсыз (0-0.4)
Ұқыптылық пен дәлдік	Толығымен стандарт бойынша және ұқыпты рәсімделген	Ұқыпты, бірақ стандартқа сәйкес емес рәсімделген	Стандартқа сәйкес емес, ұқыпты емес рәсімделген	Материал рәсімделмеген, құрылымдалмаған
Толықтығы мен жетілуі	Тапсырма толығымен және дұрыс орындалды, механикалық қателер болуы мүмкін	Тапсырма толығымен орындалды, бірақ қателер бар	Тапсырма 70% орындалды және қателер бар	Тапсырма 50% - дан аз орындалды және қателер бар
Ерекшелігі	Жұмыс толығымен түпнұсқа	Жұмыс 80% түпнұсқа	Жұмыс 60% түпнұсқа	Жұмыс түпнұсқа емес, коэффициент 0

Жалпы балл келесі формула бойынша есептеледі:

Баға = (А + Т + З)×О

12. Жұмысты кеш тапсыру саясаты

Студент дәрістер мен практикалық сабақтарға дайындалып келуі керек. Барлық жұмыс түрлерін (практикалық және өзіндік) толық орындау және уақытында қорғау талап етіледі. Студент сабақтан кешікпеуі және қалмауы қажет, жауапты және ұқыпты болуы керек. Уақытылы тапсырылмаған жұмыс үшін максималды балды 10% төмендету көзделген. Егер Сіз белгілі себептермен аралық бақылауды өткізіп алуға мәжбүр болсаңыз, онда Сіз бұл туралы оқытушыға алдын ала ескертіп, ертерек тапсыру мүмкіндігін алсаңыз болады. Емтиханды себепсіз жіберіп алу Сіздің оны қайта тапсыру құқығыңыздан айырады. Егер сіз емтиханды дәлелді себептермен жіберіп алсаңыз, қайта тапсыруға арнайы рұқсат беріліп, емтиханның күні, уақыты мен орны белгіленеді.

13. Академиялық тәртіп және этика саясаты

Басқа адамдардың пікірін құрметтеңіз, төзімді болыңыз. Қарсы пікіріңізді дұрыс қалыпта білдіріңіз. Плагиатқа және адал емес жұмыстың басқа түрлеріне жол берілмейді. Басқа студенттер үшін емтихан тапсыруға, өзгеден көшіруге, айла қолдануға жол берілмейді. Курстың кез-келген ақпаратын бұрмалған студент «F» қорытынды бағасын алады.

Дәріс және практикалық сабақтардағы *белсенділік* сіздің қорытынды балл /бағаңызға тікелей әсер етеді. Дәріс материалдарын күшейтетін көптеген теориялық сұрақтар тек дәрістерде ұсынылады. Сондықтан сабақты жіберіп алу сіздің үлгеріміңізге және сіздің соңғы бағаңызға әсер етуі мүмкін. Сабақ аяқталғанға дейін қандай да бір себептермен *екі рет* кету немесе кешігу *бір жіберілген сабақ* ретінде есептеледі. Алайда, тек сабаққа қатысу ұпайдың жоғарылауын білдірмейді. Сіздің сабақта үнемі белсенді болуыңыз қажет. Курстың міндетті талабы - әр сабаққа дайын болу. Оқулықтың көрсетілген бөлімдерін және қосымша материалдарды практикалық жаттығуларға дайындық кезінде ғана емес, сонымен бірге тиісті дәріске қатыспас бұрын да қарап шығу керек. Мұндай дайындық Сіздің жаңа материалды қабылдауыңызды жеңілдетеді және университет қабырғасында білімді белсенді түрде алуға ықпал етеді.

Пәнді оқыту аясында сыбайлас жемқорлықтың кез-келген көріністеріне жол берілмейді. Мұндай іс-шараларды ұйымдастырушы (мұғалім, студенттер немесе олардың атынан үшінші тұлғалар) Қазақстан Республикасының заңнамасын бұзғаны үшін толық жауапкершілікке тартылады.

Көмек: Өздік жұмыстарды орындау, оларды тапсыру және қорғау бойынша кеңестер, сондай-ақ өтілген материал туралы және оқылатын курс туралы барлық туындаған сұрақтар бойынша қосымша ақпарат алу үшін оқытушымен жұмыс уақытында немесе тәулік бойы электронды байланыс құралдары арқылы байланыса аласыз.

Оқу барысында

Сабақ кестесіне сәйкес міндетті түрде сабаққа қатысу студенттің сабаққа дайындығын анықтайды. Сабаққа қатыспаған жағдайда студент оқытушыға тәулік ішінде хабарлауға және сабақты өздігінен үйрену жоспарын түсіндіруге міндетті.

– оқу алдында ұсынылған материалдарды міндетті түрде оқып шығу;

– тапсырмаларды уақытында тапсыру. Кеш тапсырғаны үшін -10% айыппұлдар қарастырылған;

– 20% сабаққа қатыспау (растайтын құжаттармен дәлелді себептерімен) - «F (Fail)» бағасына тең;

– тапсырманы орындау кезінде плагиат пен алдауға жол берілмейді;

– электронды гаджеттерді сабақта қолдану рұқсат етілгенімен, емтихан кезінде пайдалануға жол берілмейді;

Пән бойынша оқыту шеңберінде академиялық әділетсіздіктің, академиялық әдепсіздіктің және академиялық алдаудың және сыбайлас жемқорлықтың кез келген нысандағы кез келген көріністеріне жол берілмейді.

Мұндай іс-әрекеттерді ұйымдастырушы (оқытушы, студенттер немесе үшінші тұлғалар олардың тапсырмасы бойынша) Қазақстан Республикасының заңдары мен университет ережелерін бұзғаны үшін толық жауапты болады.

Академиялық семестрдің басында білім алушылар силлабустың мазмұнымен танысуы қажет ҚазҰТЗУ 401-03 Ү. Таныстыру журналы.docx.

Киберқауіпсіздік кафедра отырысында қаралды және мақұлданды
2026 жылғы «28» 08 № 7 хаттама

Кафедра меңгерушісі **Ягалиева Б.Е.**

Құрастырушылар **Алимсеитова Ж.К.**
Ахмедьярова А.Т.

Келісілді:

1. **Юбузова Х.И.**
2. **Жумагалиева А.С.**