САТБАЕВ УНИВЕРСИТЕТІ SATBAYEV UNIVERSITY

Автоматика және ақпараттық технологиялар институты

Киберқауіпсіздік кафедрасы

БЕКІТЕМІН
АжАТ институтының директоры
_____ Дайнеко Е.А.
«26» 06 2026 ж.

СИЛЛАБУС

SEC2741 Кибершабуылдарды анықтау және оларға қарсы әрекет етудің интеллектуалды құралдары

7М06301 Ақпараттық қауіпсіздікті кешенді қамтамасыз ету

Пән циклі ПП, 5 (2/0/1/0) кредит

Курс 1, семестр 1

2026-2027 оқу жылы

Алматы 2026

1. 1. Оқытушы туралы ақпарат

1.1 Лектор: Ахмедиярова Айнур Танатаровна, профессор

офис: 325ГУК Офис-сағаттары: _____
e-mail: a.akhmediyarova@satbayev.university

1.2 Практикалық сабақтарды жүргізетін оқытушы:
Ахмедиярова Айнур Танатаровна, профессор

офис: 325ГУК Офис-сағаттары: _____

e-mail: a.akhmediyarova@satbayev.university

Оқу нысаны – күндізгі

2. Пререквизиттер және постреквизиттер

Пререквизиттер	Ақпаратты қорғаудың ақпараттық негіздері
Постреквизиттер	ECA212 Магистрлік диссертацияны ресімдеу және қорғау

3. Пәннің мақсаты мен міндеттері

Мақсаты: магистранттарда кибершабуылдарды интеллектуалды әдістермен анықтау, жіктеу және оларға қарсы әрекет ету қағидалары туралы жүйелі түсінік қалыптастыру, сондай-ақ киберқауіпсіздік деректерін талдау үшін машиналық және терең оқыту модельдерін әзірлеу, оқыту, бағалау және қолдану бойынша практикалық дағдыларды қалыптастыру.

Пәнді оқу келесі Тұрақты даму мақсаттарына үлес қосады:

- ТДМ 4 «Сапалы білім» – киберқауіпсіздік, деректерді талдау және жасанды интеллект саласындағы заманауи кәсіби құзыреттерді дамыту;
- ТДМ 8 «Лайықты жұмыс және экономикалық өсу» – цифрлық экономика үшін киберқауіпсіздік саласында сұранысқа ие кәсіби құзыреттерді қалыптастыру;
- ТДМ 9 «Индустрияландыру, инновациялар және инфрақұрылым» – интеллектуалды киберқорғаныс технологияларын зерттеу, әзірлеу және енгізу дағдыларын дамыту;
- ТДМ 10 «Теңсіздікті азайту» – қауіпсіз әрі қолжетімді цифрлық сервистерді құруда интеллектуалды технологияларды жауапты қолдану қағидаларын түсіну;
- ТДМ 16 «Бейбітшілік, әділдік және тиімді институттар» – ақпараттық жүйелердің сенімділігі мен тұрақтылығын арттыру, деректерді қорғау және киберқауіптерге жауапты әрекет ету мәселелерін зерттеу.

Міндеті: курс магистранттарға кибершабуылдарды анықтау мен оларға қарсы әрекет етудің заманауи интеллектуалды әдістері туралы жүйелі түсінік

қалыптастыруға және оларды киберқауіпсіздік міндеттерінде практикалық қолдану тәсілдерін меңгеруге мүмкіндік береді.

Негізгі міндеттер:

- кибершабуылдардың негізгі түрлерін, белгілерін, шабуыл векторларын және даму үрдістерін зерттеу;
- желілік трафикті, жүйелік журналдарды және киберқауіпсіздік оқиғаларын интеллектуалды талдау әдістерін меңгеру;
- кибершабуылдарды анықтау және жіктеу үшін машиналық оқыту алгоритмдерін қолдану дағдыларын қалыптастыру;
- аномалияларды, фишингті, зиянды бағдарламаларды және пайдаланушылардың күмәнді мінез-құлқын анықтау әдістерін зерттеу;
- терең оқыту модельдерін киберқауіпсіздік міндеттеріне қолдану тәсілдерін меңгеру;
- SIEM, SOAR, XDR, Threat Intelligence және MITRE ATT&CK негізіндегі интеллектуалды талдау мен автоматтандырылған әрекет ету қағидаларын зерттеу;
- машиналық оқыту модельдеріне бағытталған adversarial-шабуылдарды, олардың тәуекелдерін және қорғану әдістерін зерттеу.

4. Курстың сипаттамасы:

Курс 7М06302 – «Ақпараттық қауіпсіздікті кешенді қамтамасыз ету» білім беру бағдарламасының білім алушыларына арналған.

Курс аясында магистранттар кибершабуылдарды интеллектуалды анықтаудың негізгі ұғымдарын, әдістері мен заманауи бағыттарын, сондай-ақ желілік трафик, NetFlow, PCAP, жүйелік журналдар және киберқауіпсіздік оқиғалары сияқты деректер көздерін зерттейді. Деректерді жинау, алдын ала өңдеу, белгілерді қалыптастыру және модельдеуге дайындау тәсілдері қарастырылады.

Курс машиналық және терең оқыту әдістерін кибершабуылдарды жіктеу, аномалияларды, фишингті, зиянды бағдарламаларды және күмәнді пайдаланушы белсенділігін анықтау міндеттеріне қолдануды қамтиды. Random Forest, кластерлеу, Isolation Forest, нейрондық желілер, CNN, LSTM және автокодтаушылардың қолданылуы зерттеледі.

Ерекше назар SIEM, SOAR және XDR жүйелеріндегі интеллектуалды әрекет етуге, Threat Intelligence және MITRE ATT&CK қолдануға, сондай-ақ машиналық оқыту модельдерінің қауіпсіздігіне және Adversarial Machine Learning мәселелеріне аударылады. Практикалық жұмыстар Python және деректерді талдау кітапханалары арқылы орындалады.

5. Оқыту нәтижелері

Курсты аяқтағаннан кейін білім алушы:

Білуі тиіс:

- кибершабуылдардың негізгі түрлерін, шабуыл векторларын және оларды анықтау белгілерін;

- киберқауіпсіздік деректерінің ерекшеліктерін және оларды интеллектуалды талдауға дайындау тәсілдерін;
- машиналық оқыту әдістерінің кибершабуылдарды жіктеу мен аномалияларды анықтаудағы мүмкіндіктері мен шектеулерін;
- нейрондық желілер мен терең оқыту модельдерін киберқауіпсіздік міндеттеріне қолдану қағидаларын;
- фишингті, зиянды бағдарламаларды және пайдаланушылар мен нысандардың күмәнді мінез-құлқын анықтау тәсілдерін;
- SIEM, SOAR, XDR, Threat Intelligence және MITRE ATT&CK құралдарының интеллектуалды киберқорғаныстағы рөлін;
- машиналық оқыту модельдеріне бағытталған adversarial-шабуылдардың негізгі түрлерін;
- интеллектуалды киберқорғаныс шешімдерін қауіпсіз және жауапты қолдану қағидаларын.

Істей білуі тиіс:

- желілік трафикті, жүйелік журналдарды және киберқауіпсіздік деректерін жинау, тазалау және алдын ала өңдеу;
- кибершабуылдарды анықтау үшін маңызды белгілерді қалыптастыру және іріктеу;
- машиналық және терең оқыту модельдерін әзірлеу, оқыту, тестілеу және салыстыру;
- аномалияларды, фишингтік URL-мекенжайларды, зиянды бағдарламаларды және күмәнді белсенділікті анықтау;
- модель сапасын Precision, Recall, F1-score, ROC-AUC және қателер матрицасы арқылы бағалау;
- Threat Intelligence деректерін және MITRE ATT&CK білім базасын кибершабуылдарды талдауда қолдану;
- интеллектуалды модель нәтижелерін SIEM/SOAR/XDR ортасындағы әрекет ету сценарийлерімен байланыстыру;
- алынған нәтижелерді салыстыру, түсіндіру және киберқорғаныс шешімін негіздеу.

Дағдыларды меңгеруі тиіс:

- Python ортасында киберқауіпсіздік деректерін өңдеу және интеллектуалды талдау;
- Pandas, NumPy, Scikit-learn және киберқауіпсіздік деректерін талдау құралдарымен практикалық жұмыс істеу;
- машиналық және терең оқыту модельдерін эксперименттік зерттеу;
- ашық киберқауіпсіздік деректер жиынтықтарымен жұмыс істеу;
- кибершабуылды анықтайтын интеллектуалды модульдің прототипін әзірлеу;
- модельдің тиімділігі, тұрақтылығы және қауіпсіздігін бағалау;
- зерттеу нәтижелерін есеп, кесте, график және презентация түрінде ұсыну;
- интеллектуалды киберқорғаныс технологияларын қауіпсіз және жауапты қолдану.

6. Күнтізбелік-тақырыптық жоспар

Апта	Дәріс тақырыбы	Практикалық жұмыс тақырыбы	БӨЖ/БОӨЖ	Әдебиетке сілтеме	Тапсыру мерзімі
1	Киберқауіпсіздік, кибертұрақтылық және қазіргі кибершабуылдардың даму үрдістері	ПЖ№1. Киберқауіптерді, шабуыл нысандарын және қорғаныс шараларын талдау	Жеке семестрлік жобаның тақырыбын таңдау және міндеттерін тұжырымдау	[1], [3]	ПЖ№1
2	Кибершабуылдардың жіктелуі, іске асыру механизмдері және шабуыл векторлары	ПЖ№2. Фишинг, DDoS, зиянды БҚ және веб-шабуылдардың белгілерін салыстыру	Кибершабуылдардың жіктеу сызбасын әзірлеу	[1], [5]	ПЖ№2
3	Кибершабуылдарды анықтау және алдын алу жүйелері: IDS/IPS, сигнатуралық және аномалиялық тәсілдер	ПЖ№3. IDS/IPS жұмыс қағидаларын және анықтау белгілерін талдау	БӨЖ 1. Сигнатуралық және аномалиялық анықтау әдістерін салыстыру	[1], [6]	ПЖ№3 / БӨЖ1
4	Желілік трафикті мониторингтеу және кибершабуыл белгілерін анықтау	ПЖ№4. Wireshark/Zeek көмегімен желілік трафик белгілерін зерттеу	Желілік шабуыл индикаторларын жүйелеу	[1], [6]	ПЖ№4
5	Кибершабуылдарды анықтауда жасанды интеллект пен машиналық оқытуды қолдану	ПЖ№5. Киберқауіпсіздік деректерін ML-модельге дайындау және белгілерді іріктеу	БОӨЖ 1. Кибершабуылдарды анықтауда AI/ML қолдану бағыттарын талдау	[1], [5], [6]	ПЖ№5 / БОӨЖ 1
6	Машиналық оқыту негізінде желілік аномалияларды анықтау	ПЖ№6. Желілік трафиктегі аномалияларды жіктеу моделін құру	Модель сапасын Precision, Recall, F1-score арқылы бағалау	[6]	ПЖ№6
7	Гибридті интеллектуалды киберқауіпсіздік жүйелері: сигнатуралық талдау, AI және автоматты әрекет ету	ПЖ№7. Suricata және ML компоненттері бар гибридті анықтау сызбасын жобалау	Бірінші аралық аттестаттауға дайындық	[6]	ПЖ№7
8	Кибертұрақтылық және кибершабуылдарға қарсы кешенді әрекет ету қағидалары	ПЖ№8. Кибероқиғаға әрекет ету және жүйенің тұрақтылығын қалпына келтіру сценарийін әзірлеу	Кибертұрақтылық шараларын негіздеу	[1]	ПЖ№8
	Бірінші аралық аттестаттау				8-апта
9	Осалдықтарды анықтау және енуге	ПЖ№9. Енуге тестілеудің	БӨЖ 2. Осалдықтарды	[2], [7]	ПЖ№9 / БӨЖ2

Апта	Дәріс тақырыбы	Практикалық жұмыс тақырыбы	БӨЖ/БОӨЖ	Әдебиетке сілтеме	Тапсыру мерзімі
	тестілеудің теориялық негіздері	кезеңдері мен нәтижелерін талдау	анықтау және бағалау әдістері		
10	Ақпарат жинау, желіні сканерлеу және шабуыл бетін анықтау	ПЖ№10. Ашық порттар, сервистер және ықтимал шабуыл векторларын анықтау	Шабуыл бетінің моделін құру	[2], [7]	ПЖ№10
11	Веб-қосымшалардың шабуыл бетін және осалдықтарын анықтау әдістері	ПЖ№11. Веб-қосымшаның кіру нүктелері мен осалдық белгілерін талдау	БОӨЖ 2. Веб-қосымшалардағы осалдықтарды анықтау тәсілдерін салыстыру	[2], [7]	ПЖ№11 / БОӨЖ 2
12	Веб-қосымшаларға бағытталған кибершабуылдар және оларға қарсы әрекет ету	ПЖ№12. XSS, SQL Injection және CSRF шабуылдарының белгілері мен қорғаныс шараларын талдау	Веб-қосымшаны қорғау бойынша ұсынымдар әзірлеу	[2], [7]	ПЖ№12
13	Кибершабуылдарды мониторингтеу, талдау және интеллектуалды әрекет ету архитектуралары	ПЖ№13. Оқиғаларды жинау, корреляциялау және әрекет ету сценарийін жобалау	Кибероқиғаларды басымдық бойынша жіктеу	[1], [6]	ПЖ№13
14	Кибершабуылдарды интеллектуалды анықтау жүйелерінің тиімділігін бағалау	ПЖ№14. Анықтау дәлдігі, жалған іске қосылу және әрекет ету уақытын бағалау	БӨЖ 3. Интеллектуалды киберқорғаныс жүйесінің тиімділік көрсеткіштерін негіздеу	[5], [6]	ПЖ№14 / БӨЖ3
15	Интеллектуалды киберқорғаныс жүйелерінің даму бағыттары және кешенді қорғаныс	ПЖ№15. Семестрлік жобаны таныстыру және қорғау	Жобаның қорытынды есебін рәсімдеу	[1], [5], [6]	ПЖ№15
	Екінші аралық аттестаттау				15-апта
	Қорытынды емтихан: жазбаша			кесте бойынша	

7. Әдебиеттер

Негізгі әдебиеттер	Қосымша әдебиеттер
1. Менщиков А.А., Заколдаев Д.А., Воробьева А.А. Введение в кибербезопасность и киберустойчивость : учебно-методическое пособие. — Санкт-Петербург : Университет ИТМО, 2024. — 72 с.	5. Назарян А.К., Карцан И.Н. Современные кибератаки: классификация и способы защиты // Информатика. Экономика. Управление. — 2025. — Т. 4, № 1. — С. 1001–1007. — DOI: 10.47813/2782-5280-2025-4-1-1001-1007.

2. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение : учебно-методическое пособие. — Санкт-Петербург : Университет ИТМО, 2018. — 45 с.	6. Лукьянец С.Е. Гибридные системы кибербезопасности: искусственный интеллект и анализ сетевого трафика для противодействия современным угрозам.
3. Вострецова Е.В. Основы информационной безопасности : учебное пособие для студентов вузов. — Екатеринбург : Издательство Уральского университета, 2019. — 204 с. — ISBN 978-5-7996-2677-8.	7. Сигалов Д.А. Методы выявления поверхности атаки веб-приложений при помощи анализа клиентского JavaScript-кода : диссертация на соискание ученой степени кандидата технических наук. — Москва : МГУ имени М.В. Ломоносова, 2024.
4. Шаньгин В.Ф. Информационная безопасность : учебное пособие. — Москва : ДМК Пресс, 2014. — 702 с.	8. Кривчун Н.А., Солодовников Д.В., Соколов А.К., Шорохов К.Д., Кучук М.И. Кибератаки и методы их предотвращения в информационных системах // Дискуссия. — 2024. — Вып. 128. — С. 120–126. — DOI: 10.46320/2077-7639-2024-7-128-120-126.

8. Құзыреттер шеңбері

Оқыту дескрипторлары	Құзыреттер				
	Жаратылыстану-ғылыми және теориялық-дүниетанымдық	Әлеуметтік-жеке және азаматтық	Жалпы инженерлік-кәсіби	Мәдениетаралық-коммуникативтік	Арнайы-кәсіби
Білу және түсіну	Интеллектуалды талдаудың негізгі қағидаларын түсіну	Киберқауіпсіздіктің әлеуметтік маңызын түсіну	Кибершабуылдарды анықтау жүйелерінің құрылымын білу	Кәсіби терминологияны түсіну	ML/DL негізіндегі кибершабуылдарды анықтау әдістерін білу
Білім мен түсінікті қолдану	Деректерді талдау әдістерін қолдану	Қауіпсіздік пен жауапкершілік талаптарын ескеру	Инженерлік киберқорғаныс міндеттерін шешу	Нәтижелерді кәсіби түрде ұсыну	Интеллектуалды анықтау модельдерін әзірлеу және қолдану
Пікір білдіру және іс-әрекеттерді талдау	Модель нәтижелерін талдау және бағалау	Киберқауіптердің салдарын бағалау	Әдістерді салыстыру және шешімді негіздеу	Техникалық қорытындыларды дәлелді жеткізу	Модель тиімділігі, сенімділігі және қауіпсіздігін бағалау
Коммуникативтік және шығармашылық қабілеттер	Зерттеу нәтижелерін ұсыну	Командада жауапкершілікпен жұмыс істеу	Инновациялық шешім ұсыну	Кәсіби пікірталас жүргізу	Киберқорғаныс прототипін жобалау және қорғау

Өзін-өзі оқыту және цифрлық дағдылар	Жаңа әдістерді өздігінен меңгеру	Цифрлық технологияларды жауапты пайдалану	Бағдарламалық құралдар мен кітапханаларды қолдану	Кәсіби цифрлық ресурстармен жұмыс істеу	Киберқауіпсіздік пен AI саласындағы жаңа технологияларды өздігінен меңгеру

9. Талап етілетін жұмыстарды тапсыру кестесі

№ р/с	Бақылау түрлері	Аптадағы ең жоғары балл	Жалпы ең жоғары балл															
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Жалпы ең жоғары балл
1	Дәріс сабақтарындағы белсенділік	1	1	1	1	1	1	1	1		1	1	1	1	1	1	1	60
2	Оқытушымен білім алушының өзіндік жұмысы (БОӨЖ)	2					2								2			
3	Білім алушының өзіндік жұмысы (БӨЖ)	2			2							2						
4	Практикалық тапсырмаларды орындау	2		2	2	2	2	2	2	2	2	2	2	2	2	2	2	
5	Зертханалық тапсырмаларды орындау																	
6	1-аралық аттестаттау	5								5								
7	2-аралық аттестаттау	5															5	
8	Қорытынды емтихан*																	40
	Барлығы																	100

10. Қорытынды бақылауды бағалау

Әріптік жүйедегі баға	Баллдың сандық баламасы	Пайыздық мазмұны	Критерий	Дәстүрлі жүйедегі баға
A	4	95-100	Білімнің ең жоғары стандарттарын көрсетеді, курс көлемінен жоғары деңгейде меңгерген	«Өте жақсы»
A-	3,67	90-94	Білімнің ең жоғары стандарттарына сәйкес	
B+	3,33	85-89	Өте жақсы және жоғары білім стандарттарына сәйкес	«Қанағаттанарлық»
B	3	80-84	Жақсы және жоғары стандарттардың көпшілігіне сәйкес	
B-	2,67	75-79	Жоғары стандарттарға жақын, жеткіліктен жоғары білім	
C+	2,33	70-74	Жалпы стандарттарға сәйкес жеткілікті білім	
C	2	65-69	Жалпы білім стандарттарының	

			көпшілігіне сәйкес	«Қанағаттанарлық»
C-	1,67	60-64	Қанағаттанарлық, бірақ кейбір білім талаптарына толық сәйкес емес	
D+	1,33	55-59	Ең төменгі деңгейде қанағаттанарлық, бірқатар білім талаптарына сәйкес емес	
D	1	50-54	Күмәнді сәйкестікпен ең төменгі өту балы	
FX	0,5	25-49	Уақытша баға: қанағаттанарлықсыз, емтиханды қайта тапсыру қажет	«Қанағаттанарлықсыз»
F	0	0-24	Пәнді меңгеруге әрекет жасамаған немесе емтиханда академиялық адалдықты бұзған	

11. Бағалау критерийлері

Тест тапсырмаларынан басқа әрбір жұмыс 4 критерий бойынша бағаланады:

– ұқыптылық және дәлдік (А) – 30% (жұмыстың қаншалықты дәл және ұқыпты орындалғаны);

– шығармашылық және креативтілік (Т) – 30% (жұмыстың қалай және қандай тәсілмен ұсынылғаны);

– толықтық және жетілгендік (Ж) – 40% (жұмыстың қаншалықты терең, логикалық және құрылымды орындалғаны);

– түпнұсқалық (О) – 1.0; 0.5 немесе 0 арнайы коэффициентімен есептеледі.

Критерийлер	**Өте жақсы (0.9-1.0)**	**Жақсы (0.7-0.9)**	**Қанағаттанарлық (0.4-0.7)**	**Қанағаттанарлықсыз (0-0.4)**
Ұқыптылық және дәлдік	Жұмыс ұқыпты әрі дәл орындалған, белгіленген талаптарға толық сәйкес	Жұмыс ұқыпты орындалған, бірақ ұсақ дәлсіздіктер немесе рәсімдеу кемшіліктері бар	Жұмыс талаптарға ішінара сәйкес, дәлсіздіктер мен рәсімдеу қателері бар	Жұмыс ұқыпсыз орындалған, талаптарға сәйкес емес, елеулі қателер бар
Шығармашылық және креативтілік	Шығармашылық тәсіл көрсетілген, өзіндік идеялар мен дербес шешімдер ұсынылған	Шығармашылық тәсіл элементтері және дербес шешімдер бар	Шығармашылық тәсіл әлсіз, негізінен стандартты шешімдер қолданылған	Шығармашылық тәсіл жоқ, дербес шешімдер ұсынылмаған
Толықтық және жетілгендік	Тапсырма толық орындалған, барлық талап сақталған, нәтиже аяқталған және негізделген	Тапсырма негізінен толық орындалған, жекелеген ұсақ кемшіліктер бар	Тапсырма ішінара орындалған (шамамен 60–70%), кейбір элементтер ашылмаған немесе аяқталмаған	Тапсырманың 50%-дан азы орындалған, негізгі талаптар орындалмаған

Түпнұсқалық	Жұмыс толық дербес, өзіндік шешімдер мен авторлық тәсіл ұсынылған	Жұмыс негізінен дербес, жекелеген типтік немесе алынған шешімдер бар	Жұмыстың едәуір бөлігі дайын шешімдерге негізделген, дербес үлес шектеулі	Жұмыс дербес емес, негізінен дайын немесе көшірілген материалдар қолданылған

Жалпы баға келесі формула бойынша есептеледі:
Баға = (А + Т + Ж)×О

12. Жұмыстарды кеш тапсыру саясаты

Білім алушы дәріс және практикалық сабақтарға дайындалып келуі тиіс. Барлық жұмыс түрлерін уақтылы орындау және қорғау талап етіледі. Білім алушы сабаққа кешікпеуі және себепсіз қалдырмауы, ұқыпты әрі жауапты болуы тиіс. Белгіленген мерзімнен кейін тапсырылған жұмыс үшін ең жоғары балл 10%-ға төмендетіледі. Егер білім алушы дәлелді себеппен аралық аттестаттауға қатыса алмаса, бұл туралы оқытушыға алдын ала хабарлауы қажет. Емтиханды себепсіз өткізіп алу оны тапсыру құқығынан айырады. Дәлелді себеп болған жағдайда университет тәртібіне сәйкес емтиханның басқа күні, уақыты және орны белгіленеді.

13. Академиялық мінез-құлық және әдеп саясаты

Толерантты болыңыз, өзгенің пікірін құрметтеңіз. Қарсылықтар мен пікірлерді әдепті түрде білдіріңіз. Плагиатқа және академиялық адалдықты бұзудың басқа түрлеріне жол берілмейді. Емтихан кезінде көмек көрсетуге, көшіруге немесе басқа білім алушының орнына емтихан тапсыруға тыйым салынады. Курс бойынша ақпаратты бұрмалаған білім алушыға қорытынды «F» бағасы қойылады.

Дәріс және практикалық сабақтардағы белсенділік қорытынды бағаның құрамдас бөлігі болып табылады. Теориялық материалдың бір бөлігі тек дәрістерде қарастырылатындықтан, сабаққа қатыспау оқу нәтижесіне әсер етуі мүмкін. Сабаққа қатысудың өзі баллды автоматты түрде арттырмайды; білім алушының тұрақты белсенділігі мен әр сабаққа дайындығы талап етіледі. Ұсынылған оқу материалдарын практикалық сабақтарға ғана емес, тиісті дәріске дейін де алдын ала қарастыру қажет.

Көмек: өзіндік жұмыстарды орындау, тапсыру және қорғау, сондай-ақ пән бойынша қосымша ақпарат алу үшін оқытушының офис-сағаттарында немесе жұмыс уақытында электрондық байланыс құралдары арқылы хабарласуға болады.

Оқу барысында

Сабақ кестесіне сәйкес оқу сабақтарына міндетті түрде қатысу қажет. Сабаққа қатыспаған жағдайда білім алушы бір тәулік ішінде оқытушыға хабарлап, тақырыпты өздігінен меңгеру жоспарын түсіндіруі тиіс:

- сабаққа дейін ұсынылған материалдарды міндетті түрде оқу;

- тапсырмаларды белгіленген мерзімде тапсыру;
- аудиториялық сабақтардың 20%-ына қатыспау (дәлелді себеп және растайтын құжаттар болған жағдайда да) – «F (Fail)» бағасы;
- тапсырмаларды орындау кезінде плагиат пен көшіруге жол берілмейді;
- сабақта электрондық құрылғыларды оқу мақсатында қолдануға болады, бірақ емтиханда оларды пайдалануға тыйым салынады.

Пәнді оқу барысында академиялық адалдықты, академиялық тәртіпті бұзудың, академиялық алдаудың және сыбайлас жемқорлықтың кез келген түріне жол берілмейді. Мұндай әрекеттерді ұйымдастырушылар Қазақстан Республикасының заңнамасына сәйкес жауапкершілікке тартылады.

Ф КазНИТУ 401-03. Журнал ознакомления.docАкадемиялық семестрдің басында білім алушылар Ф ҚазҰТЗУ 401-03 «Силлабуспен танысу журналы» құжатының мазмұнымен танысуы қажет.

«Киберқауіпсіздік» кафедрасының отырысында қаралды және мақұлданды, хаттама №_7_ «_08_» _06__ 2026 ж.

Кафедра меңгерушісі **Ягалиева Б.Е.**

Құрастырушы **Ахмедиярова А.Т.**

Келісілді:

1. **Оган А.**
2. **Жумагалиева А.С.**