*«Ақпараттық қауіпсіздік криптографиялық құралдарын жобалау »*

***пәні бойынша қорытынды бақылау бағдарламасы***

***2024/2025 оқу жылы***

*күзгі семестр*

**Факультет** *Ақпараттық технологиялар факультеті*

**Кафедра** *Киберқауіпсіздік және криптология*

**Білім беру бағдарламасының коды және атауы** « 8D06303 Криптология »

**Бөлімі**: *қазақ*

**Білім беру деңгейі:** *докторант*

**Курс***: 1*

**Оқытушы**: *Омаров Б.С.*

**Қорытындыбақылауды жүргізу формасы** – *жазбаша*

**Емтихан форматы**- *офлайн*

***МОДУЛЬДЕР, ДӘРІСТЕР, СЕМИНАРЛАР НЕГІЗІНДЕ ПӘННІҢ ТАҚЫРЫПТЫҚ БАҒДАРЛАМАСЫ***

1. Криптография мен ақпараттық қауіпсіздіктің заманауи міндеттеріне кіріспе.
2. Кванттық криптографияның математикалық негіздері мен теориялық аспектілері.
3. Торлы Криптография: кванттық шабуылға төзімділік және қолдану.
4. Алгебралық топтар теориясы және эллиптикалық қисықтардың криптографияда
5. Толық гомоморфтық шифрлау әдісі және оның бұлттық есептеулерде деректер құпиялығын қорғаудағы рөлі.
6. Көпқырлы криптографиялық жүйелер, мультибазистік кілттер және олардың қауіпсіздікке қосар үлесі.
7. Қауіпсіз көпжақты есептеулер (MPC) және олардың деректерді құпия түрде өңдеудегі қолданбалы маңызы.
8. Нөлдік білім дәлелдемелері және олардың аутентификация және блокчейн жүйелеріндегі рөлі.
9. Посткванттық криптографияның негізгі әдістері, кодтық және мультимерлік криптографияның болашағы.
10. Кванттық криптоанализ: кванттық шабуылдар, алгоритмдер, қарсы қорғаныс шаралары.
11. Бүйірлік арналар арқылы шабуыл жасау әдістері және қауіпсіздік шаралары.
12. Бұлттық және бөлінген жүйелерде қолданылатын криптографиялық қауіпсіздік шаралары.
13. Блокчейн технологияларындағы криптографиялық әдістер және деректердің өзгермейтіндігін қамтамасыз ету.
14. Жасанды интеллекттің криптоанализдегі рөлі және қауіпсіздікке тигізетін әсері.
15. Ақпараттық қауіпсіздік криптографиясының болашағы: кванттық және жасанды интеллектпен қақтығысқан кездегі проблемалар мен перспективалар.

***ТАҢДАЛҒАН ФОРМА БОЙЫНША ҚОРЫТЫНДЫ БАҚЫЛАУ ТАПСЫРМАСЫН ОРЫНДАУҒА АРНАЛҒАН ӘДІСТЕМЕЛІК НҰСҚАУЛАР***

**Стандартты емтихан:** *жазбаша*

**Емтихан форматы–** *офлайн***.**

Пән бойынша емтихан сұрақтарының жалпы саны: 15

Бұл форма білім алушының жауаптары мен ережелерінің дәлелдерін жазбаша баяндау, дәлелдер келтіру, білім алушының коммуникативтік құзыреттілігін дамытуға ықпал ететін пәндер бойынша қорытынды бақылауға арналған. Емтиханның бұл формасында емтихан комиссиясы мен студент арасында тікелей байланыс орнатылмайды, оның барысында білім алушы оқу материалын меңгеру деңгейін көрсетеді. Аппараттық/бағдарламалық жасақтаманы әзірлеу бойынша практикалық тапсырмаларды орындау аппараттық модульдерді құрастыру және іске қосу үшін компьютерлерді, зертханалық жабдықты пайдалануды қамтиды.

Жеке жауаптарында оқу материалына қатысты сұраққа мұқият, дәйекті жауаптарын қамтиды, сондықтан ол білім алушылардың есте сақтау қабілетін, ойлауын, білімін жеткізудің маңызды құралы ретінде қызмет етеді.

Бұл форманы қолдану сонымен қатар топтың барлық студенттерінің оқу материалын игеруін бір уақытта тексеруге, барлығына бірдей талаптар қоюға мүмкіндік береді, бұл оқу нәтижелерін бағалаудың объективтілігін арттырады

-

***НҰСҚАУЛЫҚ БОЙЫНША ЖҰМЫСТЫҢ НЕГІЗГІ КЕЗЕҢДЕРІ***

**Жазбаша емтиханның *ұзақтығы*** – 2сағат.

Емтихан билеті 3 сұрақтан тұрады: 2 теориялық сұрақ, 1 практикалық сұрақ.

Әрбір сұрақ бойынша тиісті максималды балл жақшада пайызбен көрсетіледі.

*Жазбаша офлайн емтиханды ұйымдастыру*

1. Офлайн жазбаша емтихан басталардан 15 минут бұрын кезекші оқытушы жеке куәліктері арқылы білім алушыларды тексереді және білім алушыларды емтиханға қатысу парағында көрсетілген орындарға отырғызады.

2. Офлайн жазбаша емтиханға білім алушының орнына басқа адам келген жағдайда, кезекші оқытушы емтихан тапсыру қағидаларының бұзылғаны туралы тиісті хаттама жасайды.

3. Кешіккен студенттер емтиханға жіберілмейді.

**Емтихан тапсыруға қойылатын талаптар:**

- бекітілген кестеге сәйкес;

- студент кез келген ретпен сұрақтарға жауап бере алады.

- рұқсат етілмеген материалдардың пайдаланылуы немесе студенттердің басқа кеңестер алуы, білім алушылардың жұмысында арнайы белгілері (мысалы, студенттің аты-жөні, арнайы белгілер және сәйкестендірулер) қалдырылғаны анықталса, емтихан жойылуы мүмкін.

**БАҒАЛАУ САЯСАТЫ- БАҒАЛАУ РУБРИКАТОРЫ**

**ҚОРЫТЫНДЫ БАҚЫЛАУДЫ КРИТЕРИАЛДЫ БАҒАЛАУ РУБРИКАТОРЫ**

**Пән**: *Ақпараттық қауіпсіздік криптографиялық құралдарын жобалау*.

**Форма:** *жазбаша***. Платформа:** *офлайн*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Балл  Критерийі | ДЕСКРИПТОРЛАР | | | | |
| «Өте жақсы» | «Жақсы» | «Қанағаттанарлық» | «Қанағаттанарлықсыз» | |
| 90-100 % | 70-89% | 50-69% | 25-49% | 0-24 % |
| 1 сұрақ | Курстың теориясы мен тұжырымдамасын білу жəне түсіну | Сұрақтарға толық жауаптар берілген, қажет болған жағдайда көрнекі мысалдармен суреттелген, ақпараттық қауіпсіздік криптографиялық құралдарын жобалау. программа жазылған; жауаптар сауатты ғылыми тілде баяндалған, барлық операторлар мен командалар, ұғымдар дұрыс қолданылған жəне дұрыс ашылған. | Сұрақтарға тұтастай дұрыс жауаптар берілді, бірақ принципті емес жеке дəлсіздіктермен берілді. Барлық ақпараттық қауіпсіздік криптографиялық құралдарын жобалау. операторлары мен командалары, терминдері дұрыс қолданылмайды, жеке қате мəлімдемелер жəне презентацияның грамматикалық / стилистикалық қателіктері бар. Жауаптар мысалдармен дұрыс көрсетілмеген. | Сұрақтарға жауаптар реферативті сипатта болып табылады, дұрыс тұжырымдар дұрыс емес тұжырымдармен қиылысады. Тақырыпты толық ашу үшін қажетті ақпараттық қауіпсіздік криптографиялық құралдарын жобалау. блоктары келтірілмеген. Студент жалпы оқу курсының тақырыбына назар аударады, бірақ нақты мәселелерді ашуда қиындықтарға тап болады. | Жауаптар сұрақтардың мазмұнына сəйкес келмейді. Оқу курсы үшін сұрақтардағы негізгі ұғымдар қате түсіндіріледі. | Сұрақтарға жауаптар жоқ; студенттің оқу материалының көп немесе маңызды бөлігін білмеуі немесе түсінбеуі анықталды.  Қорытынды бақылау жүргізу ережелерін бұзу. |
| 2 сұрақ | Таңдалған əдістеме мен технологияны нақты қолданбалы тапсырмаларға қолдану | Курстың технологиясы мен əдістемесі білім алушыларды даярлау бағытының ерекшелігін ескере отырып, терең мағынада қолданылады; негізгі проблеманы логикалық жəне дəлелді түрде алгоритммі, соның ішінде блок схеманың көмегімен дұрыс көрсетеді; | Курстың əдістемесі мен студенттің алған білімі əлсіздеу интеграцияланған жəне кейбір ұсынылған нақты практикалық мəселелерді шешуге бейімделген. Студенттің білімі бейімделген; жауаптардың алгоритмі, блок схеманың көмегімен əлсіз құрылымдалған, жауапта маңызды емес нақты қателіктер бар, олар жетекші сұрақтың арқасында өздігінен түзете алады; | Курстың құралдары үстірт қолданылады, мазмұны аз, жауап алгоритмінде дəлсіздіктер бар, блок схема логикасы бұзылған, ұсынылған материалдың мағынасы жоқ, пəнаралық байланыстар туралы түсінік жоқ. | Пəннің маңызды бөлігін дұрыс қолданбайды, студент өздігінен түзете алмайтын елеулі нақты қателіктерге жол береді, емтихан мазмұны бойынша қосымша сұрақтардың көпшілігіне жауап беру қиынға соғады немесе ол дұрыс жауап бермейді. | Жауап беру кезінде (бір сұраққа) 3-4-тен астам өрескел қателіктер жібереді, оны ОПҚ көмегімен де түзете алмайды; материалды толық игермеген.  Қорытынды бақылау жүргізу қағидаларын бұзу. |
| 3 сұрақ | Таңдалған əдістеменің ұсынылған практикалық тапсырмаға қолданылуын бағалау жəне талдау, нəтижені негіздеу | Ақпараттық қауіпсіздік криптографиялық құралдарын жобалау. белгілі бір тақырыбы бойынша əдістер мен технологияларды интеграциялау, негіздеу жəне талдау, жауапты құрылымдау, емтихан билеті бойынша қолданыстағы теорияларды талдау қабілетінің болуы, жауаптар мысалдармен жəне көрнекі материалдармен, программа кодын жазу; диалог жүргізу жəне ғылыми пікірталасқа түсу қабілетін көрсетеді. | Білімді жаңғырту кезінде елеусіз қателіктер жібере отырып, ақпараттық қауіпсіздік криптографиялық құралдарын жобалау. программалау тілінің операторлары мен командалары қолдану арқылы өз пайымдауларын бекіту үшін көрнекі материалдарды кейіннен пайдалана отырып, курстың әдістері мен технологияларын қолдануды интеграциялау және талдау; емтихан билеті мәселесі бойынша теориялардың, практикалық мәселелердің ережесін талдау. | Ақпараттық қауіпсіздік криптографиялық құралдарын жобалау. программалау тілінің операторлары мен командалары мен принциптерінің Үстірт негіздемесі, оқу бағдарламасына сəйкес материалдың негізгі көлемін оның кейбір қиындықтармен жəне жетекші сұрақтардың талабымен əлсіз қолдану; | Курстың әдістері мен технологияларын қолданудың негізділігі мен талдауының болмауы, репродуктивті сипаттағы сұрақтарға жауап беру кезінде қиындықтың көрінісі. | Мысалдар келтіруде, көрнекі материалдарды қолдануда курс әдістемесін қолдану қабілетінің болмауы;  Қорытынды бақылау жүргізу қағидаларын бұзу. |

***ПАЙДАЛАНЫЛҒАН ДЕРЕККӨЗДЕРДІҢ ТІЗІМІ***

1. Albrecht, M. (2021). Cryptography Engineering: Design Principles and Practical Applications. Wiley.
2. Misra, S., & Roy, P. (2023). Advances in Cryptography and Network Security. Springer.
3. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2022). Handbook of Applied Cryptography (2nd ed.). CRC Press.
4. Омассон Ж.-Ф. О криптографии всерьез / пер. с  англ. А.  А.  Слинкина.  – М.: ДМК Пресс, 2021. – 328 с.: ил.
5. Gupta, M., & Saxena, A. (2024). Post-Quantum Cryptography: Theory and Practice. Springer.
6. Liu, J., & Zhou, S. (2023). Quantum-Safe Cryptography: Algorithms and Protocols for the Post-Quantum World. CRC Press.
7. Chen, L., & Chen, M. (2022). Advanced Cryptography in Digital Networks. Wiley.
8. Bhargava, B. (2021). Blockchain and Cryptography: A Comprehensive Introduction. Springer.