**әл-Фараби атындағы Қазақ ұлттық университеті**

**Ақпараттық технологиялар факультеті**

**«5В100200 – Ақпараттық қауіпсіздік жүйелері»**

**мамандығы бойынша білім беру бағдарламасы**

**Cиллабус**

**(IOZI2206) Ақпаратты қорғаудың ақпараттық негізі**

**Күзгі семестр 2019/2020 уч. год**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Пән коды | Пәннің аты | Тип | Апта бойынша сағат саны | | | | Кредиттер саны | | ECTS |
| Дәріс | Практ/семин | | Зертханалық |
| IOZI2206 | Ақпаратты қорғаудың ақпараттық негізі | ЭК | 1 | 1 | |  | 2 | | 5 |
| Дәріскер | Хомпыш АрдабекСтарший преподаватель | | | | Офис-сағаты | | | Кесте бойынша | |
| e-mail | ardabek@mail.ru | | | |
| Телефоны | 87072433362 | | | | Аудитория | | | 122 | |
| Практ/семинар /зертхана сабағын жүргізетін оқытушы |  | | | |  | | |  | |
| e-mail |  | | | |  | | |  | |
| Телефоны |  | | | | Аудитория | | |  | |

|  |  |
| --- | --- |
| Академиялық курс презентациясы | **Курстың мақсаты:** Компьютерлік жүйе мен желілерде ақпаратты қорғаудың қазіргі кездегі құралдары мен принциптерін оқу болып табылады.  Пәнді оқу нәтижесінде студенттер:  - түрлі криптожүйедегі стандарттарды қолдануға дағдылануы керек;  - криптографиялық хаттамалармен жұмыс істеуді үйренуі керек;  - вирусқа қарсы қорғанысты ұйымдастыра білуі қажет.  қабілетті болады. |
| Пререквизиттер және постреквизиттер | 1. Пән Жоғарғы оқу орында оқылатын «Ақпараттану», «Алгоритімдік тілдерде программалау» пәндерінен алынған білімге негізделеді. |
| Әдебиеттер және ресурстар | **Әдебиеттер**:  *Негізгі*:   1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах, Издательство «Советское радио» Москва, 1968. 438 б. 2. Рожков А.В., Ниссенбаум О.В. Теоретико-числовые методы в криптографии , Тюмень 2007.-175б. 3. Фомичев В.М. Симметричные криптосхемы. Краткий обзор основ криптологии для шифрсистем с открытым ключом. — М.: МИФИ, 1995. 4. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. — М.: Высшая школа, 1999. 5. Синьков М.В., Губарени Н.М. Непозиционные представления многомерных числовых систем. Киев, Наукова думка, 1977, 149 б. 6. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005. 7. Диффи У., Хеллмэн М.Э. Защищенность и имитостойкость: введение в криптографию. // ТИИЭР N 3, т. 67, 1979 г., б.71-109. 8. Хоффман Л.Д. Современные методы защиты информации / Под ред. В.А. Герасименко. – М.: Сов. радио, 1980. – 264 б. 9. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Издательство ТРИУМФ, 2002 - 816 с.: ил. 10. Алферов А.П., Зубов А.Ю., Кузьмин А.С. и др. Основы криптографии. – М.: Гелиос АРВ, 2001. – 122 б. 11. Фомичев В.М. Дискретная математика и криптология. – М.: ДИАЛОГ-МИФИ, 2003. - 400 б. 12. А.Ж. Асамбаев., Криптография негіздері, Оқу құралы. – Павлодар, 2012. – 173 бет.   *Қосымша*  1. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.   1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999. 2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2002. – 480 с.     **Интернет-ресурстар:**  1. intuit.ru  2.Қосымша оқу материалдары, сонымен қатар үй тапсырмалары мен жобаны орындауға пайдаланылатын қажетті құжаттамалар univer.kaznu.kz сайтының ПОӘК бөлімінде студенттерге қолжетімді. |
| Университеттің моральдық-этикалық құндылықтарына сай курстың академиялық саясаты | **Академиялық ереженің тәртібі:**  Студенттер сабақтарға міндетті түрде кешікпей қатысуы керек, сабаққа себепсіз қатыспауға болмайды. Сабаққа себепсіз қатыспаса, кешігіп келсе 0 бал қойылады.  Тапсырмаларды (СӨЖ бойынша, аралық бақылау, зертханалық, практикалық/семинарлық, жоба жұмыстарын және т.б), қорытынды емтиханды уақытында орындауға және тапсыруға міндетті.  Тапсырмаларды орындап, тапсыру барысында студент тапсыру мерзімін бұзған жағдайда жоспарланған максималды балдан айыппұл (50%) шегеріліп, бағаланады.  **Академиялық құндылықтар:**  Академиялық құндылық және адалдық: барлық тапсырмаларды өз бетінше орындау; плагиатқа, жалғандыққа, шпаргалканы пайдалануға жол бермеу, білімді бақылаудың барлық кезеңінде көшіруге, оқытушыны алдау және оған деген қарым-қатынасының нашарлығын болдырмау (ҚазҰУ студенттерінің ар-намыс кодексі).  Мүмкіндігі шектеулі студенттер арнайы ardabek@mail.ru бойынша көмек ала алады. |
| Бағалау саясаты және аттестаттау | **Критериалды бағалау:**  Орындалған жұмыстар менқорытынды емтихан барысында теориялық материалдың меңгерілуі мен теориялық және практикалық дағдыларды қабылдауы дескрипторға сәйкес тексеріледі (аралық бақылау мен емтиханда құзыреттіліктің қалыптасуын тексеру).  **Жиынтық бағалау:** аудиториядағы жұмыс белсенділігі, қатысуы және орындалған тапсырма бағаланады. Қорытынды баға төменде келтірілген білімді бағалау шкаласына сәйкес қойылады. |

**Білімді бағалау шкаласы**

|  |  |  |  |
| --- | --- | --- | --- |
| Әріптік жүйе бойынша бағалау | Балдардың сандық эквиваленті | Балдар (%-дық қатынаста) | Дәстүрлі жүйе бойынша бағалау |
| А | 4,0 | 95-100 | Өте жақсы |
| А- | 3,67 | 90-94 |
| В+ | 3,33 | 85-89 | Жақсы  Қанағаттанарлық |
| В | 3,0 | 80-84 |
| В- | 2,67 | 75-79 |
| С+ | 2,33 | 70-74 |
| С | 2,0 | 65-69 |  |
| С- | 1,67 | 60-64 |
| D+ | 1,33 | 55-59 |
| D- | 1,0 | 50-54 |
| FX | 0,5 | 25-49 | Қанағаттанарлықсыз |
| F | 0 | 0-24 |

**Оқу курсының мазмұнын жүзеге асыру күнтізбесі (графигі)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Апта** | **Тақырыптың атауы** | **Сағат саны** | **Максималды балл** |
| 1 | **1-дәріс.** Негізгі түсініктер. Криптографияның дамуының қысқаша тарихы**.** | 1 | 2 |
| **1-семинар сабақ.** Классикалық симметриялы криптожүйелер | 1 | 10 |
| 2 | **2-дәріс.** Ақпаратты өңдеудің автоматтық жүйесінің (АӨАЖ) қауыпсыздігінің негізгі қауыпы. Ақпаратты қоғаудың криптографиялық принциптері. | 1 | 2 |
| **2-семинар сабақ.** Классикалық симметриялы криптожүйелер | 1 | 10 |
| **СОӨЖ 1.** «Ақпаратты қорғаудың криптографиялық әдісі» бойынша коолоквиум | 1 | 10 |
| 3 | **3-дәріс.** Классикалық симметриялы криптожүйелер. | 1 | 2 |
| **3-семинар сабақ.** Жалғанкездейсоқ сандар тізбегін генерациялау әдісін үйрену | 1 | 10 |
| **СОӨЖ 2.** «Жалғанкездейсоқ сандар тізбектерін генерациялайтын сызықты рекурентті қатынастар әдісі» бойынша реферат тапсыру | 1 | 15 |
| 4 | **4-дәріс.** Гамма тәсілі арқылы шарт белгілеу. | 1 | 2 |
| **4- семинар сабақ.** Жалғанкездейсоқ сандар тізбегін генерациялау әдісін үйрену | 1 | 10 |
| 5 | **5-дәріс.** Қазіргі симметриялы криптожүйелер. Мәліметтерді DES Американдық стандарт арқылы шарт белгілеу | 1 | 2 |
| **5-семинар сабақ.** DES алгоритмінің жұмысын үйрену. | 1 | 10 |
| **СОӨЖ 3**. «DES алгоритмі» бойынша тест жүргізу | 1 | 15 |
| **1-АБ** |  | **100** |
| 6 | **6-дәріс.** Мәліметтерді Ресей стандарт арқылы шарт белгілеу | 1 | 2 |
| **6- семинар сабақ.** ГОСТ 28147-89 алгоритмінің жұмысын үйрену. | 1 | 10 |
| 7 | **7-дәріс.** AES – RIJNDAEL | 1 | 2 |
| **7- семинар сабақ.** Rijndael алгоритмінің жұмысын үйрену. | 1 | 10 |
| **СОӨЖ 4**. Блоктық шифрларды қолдану режимі. |  | 10 |
| 8 | **8-дәріс.** Ағымды шифрлар | 1 | 2 |
| **8-семинар сабақ.** Ассиметриялық криптожүйелерде мәліметтерді шифрлау әдістерін үйрену. | 1 | 10 |
| 9 | **9-дәріс.** Криптографияда қолданатын сандар теориясының элементтері | 1 | 2 |
| **9- семинар сабақ.** Қалдықтықтар туралы Қытай теоремасы | 1 | 10 |
| **СОӨЖ 5**. «Модулярлық арифметика» қабылдау |  | 15 |
| 10 | **10-дәріс.** Асимметриялық криптожүйелер. Мәліметтерді шарт белгілеу криптожүйелері (RSA, Эль-Гамаль алгоритмі) | 1 | 2 |
| **10- семинар сабақ.** RSA, Эль-Гамаль алгоритмі | 1 | 10 |
| **СОӨЖ 6**. «RSA криптожүйесінде шифрлау және шифрды алу процедуралары» қабылдау | 1 | 15 |
| **АБ (МТ)** |  | **100** |
| 11 | **11-дәріс.** Аутентификациясы және электронды- сандық қолтаңба | 1 | 2 |
| **11- семинар сабақ.** Хештау және ЭСҚ алгоритмінің жұмысын үйрену. | 1 | 10 |
| **СОӨЖ 7**. «Бір бағыттағы хэш-функциялар» бойынша консультация беру | 1 | 10 |
| 12 | **12-дәріс.** Криптографиялық кілттермен басқару | 1 | 2 |
| **12- семинар сабақ.** Кездейсоқ сандар тізбегі арқылы кілттерді генерациялау. | 1 | 10 |
| 13 | **13-дәріс.** Internet желісі арқылы шеттелген жабуылдан қорғану әдістері және тәсілдері | 1 | 2 |
| **13-зертханалық сабақ.** Аудентификатция және идентификация. | 1 | 10 |
| **СОӨЖ 8**. «Internet желісі арқылы электрондық төлемдердің қауіпсіздігін қамтамасыз ету.» бойынша бақылау жүргізу | 1 | 15 |
| 14 | **14-дәріс.** Зерттеуден программаларды қоғау | 1 | 2 |
| **14- семинар сабақ.** Программаларды қорғау әдістерін үйрену. | 1 | 10 |
| 15 | **15-дәріс.** Антивирустық қорғау | 1 | 2 |
| **15- семинар сабақ.** Ақпараттарды антивирус арқылы қорғау әдістерін үйрену | 1 | 10 |
| **СОӨЖ 9**. «Вирустардың ақпараттарға шабулдау түрлері» қорғау | 1 | 15 |
| **2 АБ** |  | **100** |
|  | **Қорытынды емтихан** |  | **100** |
|  | **БАРЛЫҒЫ** (1АБ+АБ(МТ)+2АБ)/3х0,6+(ҚЕх0,4) |  | **100** |

Әдістемелік бюроның төрайымы Гусманова Ф.Р.

Кафедра меңгерушісі Мусиралиева Ш.Ж.

Дәріскер Хомпыш А