**СИЛЛАБУС**

**Күзгі семестр 2021-2022 оқу жылы**

**“Радиотехника, электроника және телекоммуникациялар”**

**білім беру бағдарламасы бойынша**

**4 курс**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Пән коды** | **Пәннің атауы** | **Студенттің өздік жұмысы (СӨЖ)** | **Сағат саны** | **Кредит саны** | **Оқытушының жетекшілігімен студенттің өзіндік жұмысы (СРСП)** |
| **Дәріс (Д)** | **Практ. Сабақтар (ПС)** | **Лаб. сабақтар (ЛС)** |
|  | Телекоммуникациядағы ақпараттық қауіпсіздік | 98 | 15 | - | 30 | 5 | 7 |
| **Курс туралы академиялық ақпарат** |
| **Оқыту түрі** | **Курс түрі** | **Дәріс түрі** | **Практикалық сабақтың түрі** | **СӨЖ саны** | **Қорытынды емтихан түрі** |
| Дәріс – офлайнПрактикалық сабақ - офлайн | Теориялық | Проблемалық, аналитикалық | Мәселелерді шешу, кодтарды жазу | 6 | Жазбаша емтихан |
| **Лектор** | Иманбаева Ақмарал Каримовна | Оф./сағ.Кесте бойынша |
| e-mail | AkmaraЛ.Imanbaeva@kaznu.kz |
| Telephone number | 3773346 |

|  |
| --- |
| **Академиялық курстың презентациясы** |

|  |  |  |
| --- | --- | --- |
| **Пәннің мақсаты** | **Оқытудан күтілетін нәтижелер (ОН)**Пәнді оқу нәтижесінде магистрант: | **Жетістік көрсеткіштері (ЖК)** |
| желі қауіпсіздігі мен мониторингінің негізгі принциптерін үйрену | **ОН 1** ақпараттық қауіпсіздікке қатысты негізгі ұғымдар мен анықтамаларды, ашық кілт инфрақұрылымының негізгі ұғымдарын тізіп шығу; қауіпсіз АТ-инфрақұрылымын құру принциптерін, қолданбалы және желілік деңгейлердің негізгі туннельдеу технологияларын, желіаралық қалқандардың классификациясын, енуді анықтау және алдын алу жүйелерінің классификациясы; | **ЖК** **1.1** Телекоммуникациялық жүйелерге, қызметтерге және қауіпсіздік механизмдеріне қауіп төндіретін қауіптерді жіктеу;**ЖК** **1.2** желі деңгейінде ақпарат алмасу хаттамаларын білу;**ЖК** **1.3** Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы заңнамалық және нормативтік құқықтық базасын білу. |
| **ОН 2** негізгі симметриялық және асимметриялық шифрлау алгоритмдерін, криптографиялық хэш функцияларын және хабарламаның аутентификация әдістерін қолдану; | **ЖК** **2.1** Құпия мәтіндік ақпаратты кодтау үшін кестелік әдістерді қолдану;**ЖК** **2.2** криптографияда қолданылатын сандар теориясының кейбір мәселелерін шеше білу;**ЖК** **2.3** құпия ақпаратты кодтаудың классикалық криптографиялық әдістерін қолдану: симметриялық және асимметриялық шифрлау. |
| **ОН 3** различать политики межсетевых экранов и систем обнаружения проникновений; | **ЖК** **3.1** Цифрлық қауіпсіздік сертификаттарын және оларды қолдану мүмкіндіктерін білу;**ЖК** **3.2** енуді анықтау жүйесінің (IDS) құралдарын оқу. |
| **ОН 4** определить приоритеты решений сетевой безопасности, которые устраняют множество угроз в сетях. | **ЖК** **4.1** Криптоталдау әдістерін және криптоталдау қажеттілігін білу; криптографиялық хэш функцияларын білу;**ЖК** **4.2** ақпаратты қорғаудың классикалық және заманауи алгоритмдерінің криптоталдау әдістерін қолдану. |
| **Пререквизит** | IKT2104 Ақпараттық және коммуникациялық технологиялар, М1202 Математика, ORT2212 Радиотехника және телекоммуникация негіздері, TCS3218 Сандық байланыс технологиясы |
| **Постреквизит** | Дипломдық жұмыс |
| **Әдебиеттер мен ресурстар** | 1. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие для вузов.- М.: Академия, 2005.- 254, [2] с.
2. Молдовян, А. А. и др. Криптография: Учеб..- СПб.: Лань, 2001.- 218, [6] с.
3. Нечаев, В.И. Элементы криптографии: (Основы теории защиты информации).- М.: Высш. шк., 1999.- 108, [1] с
4. Беляев А.В. Курс лекций по «Методы и средства защиты информации». <http://citforum.ru/internet/infsecure/index.shtml>
5. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000..
6. Домарев, В.В. Защита информации и безопасность компьютерных систем /.- Науч.-попул. изд.- Киев: СОФТ, 1999.- 453, [26] с
7. Галочкин, А.И. Введение в теорию чисел: Учеб. пособие - 2-е изд.- М.: МГУ, 1995.- 158, [2] c

**Онлайн қолжетімді:** Үй тапсырмасы мен СӨЖ бойынша қосымша оқу материалы univer.kaznu.kz сайтындағы UMKD бөлімінде парақшаңызда қолжетімді болады.**Интернет-ресурстар**<https://refdb.ru/look/1214614.html> - «Ақпараттық қауіпсіздік негіздері» тақырыбындағы дәрістер<http://www.4stud.info/networking/network-security.html> Желі қауіпсіздігінің негіздері. Желі қорғау объектісі ретінде<https://www.fortinet.com/ru/solutions/enterprise-midsize-business/network-security> - Желінің қауіпсіздігін анықтау және түсіндіру<https://www.owasp.org/index.php/Main_Page> - осалдықтардың деректер базасы.<https://intuit.ru/studies/courses/102/102/lecture/2971> - INTUIT желілік қауіпсіздік бойынша дәрістер |

|  |  |
| --- | --- |
| **Курстың академиялық саясаты университеттік моральдық -этикалық құндылықтар контекстінде** | **Академиялық тәртіп ережелері:**Барлық студенттер MOOC -қа тіркелуі керек. Пәнді оқу кестесіне сәйкес онлайн -курстың модульдерін толтыру мерзімі қатаң сақталуы тиіс.НАЗАР АУДАРЫҢЫЗ! Белгіленген мерзімдерге сәйкес келмеу ұпай жоғалтуға әкеледі! Әрбір тапсырманың орындалу мерзімі оқу курсының мазмұнын жүзеге асыру күнтізбесінде (кестесінде), сондай -ақ МООК -та көрсетілген.**Академиялық құндылықтар:**- Семинарлар, МӨЖ тәуелсіз, шығармашылық болуы керек.- Плагиат, жалған құжат жасау, бақылау парақтарының қолданылуы, бақылаудың барлық сатыларында алдау жол берілмейді.- Мүмкіндігі шектеулі студенттер AkmaraЛ.Imanbaeva@kaznu.kz электронды поштасы бойынша консультациялық көмек ала алады |
| **Бағалау және аттестаттау саясаты** | **Критериалды бағалау:** дескрипторларға қатысты оқу нәтижелерін бағалау (аралық бақылау мен емтихандарда құзыреттіліктердің қалыптасуын тексеру).**Жиынтық бағалау:** сабақтағы жұмыс белсенділігін бағалау; орындалған тапсырманы бағалау.Төменде пайыздық көрсеткіштер бойынша минималды бағалар берілген:95% - 100%: А 90% - 94%: А-85% - 89%: В+ 80% - 84%: В 75% - 79%: В-70% - 74%: С+ 65% - 69%: С 60% - 64%: С-55% - 59%: D+ 50% - 54%: D- 0% -49%: F Қорытынды баға формула бойынша есептеледі$$\frac{РК1+РК\left(мидтерм\right)+РК2}{3}∙0.6+0.4ИК$$ |

**Оқу курсының мазмұнын жүзеге асыруға арналған күнтізбе (кесте)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Апта  | Тақырып атауы | ОН | ЖК | Сағат саны | Максималды балл | Білімді бағалау формасы | Сабақтың формасы |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | **Д.1. Кіріспе.** Ақпараттық қауіпсіздіктің жалпы түсінігі, оның қысқаша даму тарихы. Ақпараттық қауіпсіздіктің негізгі компоненттері | ОН 1 | ЖК 1.1. | 1 |  |  | дәріс |
| **ПС.1.** Ақпараттық қауіпсіздіктің заманауи стандарттары | ОН 1  | ЖК 1.1. | 1 | 15 | TK 1 | Workshop  |
| Сенбі 23.00 - ТК 1, тапсырудығ мерзісі  |
| 2 | **Д.2.** Қауіпсіздік қатерлері. Қауіптердің классификациясы. | ОН 1 | ЖК 1.1. | 1 |  |  | дәріс |
| **ПС.2.** Шифрлау кестелері. Орын ауыстыру шифрлары. Қосарлы ауыстыру. | ОН 1  | ЖК 1.1. | 1 | 15 | TK 2 | Workshop  |
| Сенбі 23.00 - ТК 2, тапсырудығ мерзісі |
| 3 | Д.3. Қызметтер мен қауіпсіздік механизмдері. Желі деңгейіндегі ақпарат алмасу хаттамалары. | ОН 1 | ЖК 1.1ЖК 1.2 | 1 |  |  | дәріс |
| **ПС.3.** Trisemus шифрлау кестелері. Vigenere шифрлау жүйесі | ОН 1 | ЖК 1.2. | 1 | 10 | TK 3 | Workshop  |
| **СРСП 1.** СӨЖ бойынша консультация |  |  |  |  |  | office hours |
| **СӨЖ 1.** Тақырып «Сенімді және қауіпсіз АТ-инфрақұрылымын құрудың негізгі принциптері»(формасы: ауызша: сұрақтарға жауап беру) | ОН 1 | ЖК 1.2 |  | 20 | IT 1  | office hours |
| Сенбі 23.00 - ТК 3, СӨЖ 1тапсырудың мерзімі |
| 4 | **Д.4.** Желілік шабуылдардың классификациясы. Шабуылдардың категориялары және олардың анықтамалары, оларды жүзеге асыру шарттары. Шабуыл механизмі | ОН 1 | ЖК 1.1ЖК 1.2 | 1 |  |  | дәріс |
| **ПС.4.** Қос Уитстон алаңы. Playfair биграмма шифры. | ОН 1 | ID 1.2. | 1 | 20 | TK 4 | Workshop  |
| Сенбі 23.00 – ТК4 тапсырудың мерзімі |
| 5 | **Д.5.** Криптографиялық қауіпсіздік механизмдері. Криптографияның негізгі міндеттері мен түсініктері. Ақпаратты криптографиялық қорғаудың принциптері. | ОН 1 | ID 1.1. | 1 |  |  | дәріс |
| **ПС.5.** Сандар теориясының элементтері. GCD және салыстыру (кейс-тапсырма әдісі). Криптографиялық есептерді шешуге арналған Ферма және Эйлер теоремалары. | ОН 1 | ЖК 1.2. | 1 | 20 |  | Workshop  |
| Сенбі 23.00 - ТК 5тапсырудың мерзімі |
| **CW 1** |  |  |  | **100** |  |  |
| 6 | **Д.6.** Ақпараттық қауіпсіздік мәселелерінде симметриялық және асимметриялық шифрлау. | ОН 1 | ЖК 1.1ЖК 1.2 |  |  |  | дәріс |
| **ПС.6.** Кілтті тасымалдаусыз криптожүйе. Кілттерді тасымалдаусыз криптожүйедегі есептерді шешу | ОН 2  | ЖК 2.1. | 1 | 15 | TK 6 | Workshop  |
|  |  |  |  |  |  |  |
| **СРСП 2.** СӨЖ2 бойынша консультация |  |  |  |  |  | office hours |
| **СӨЖ 2.** Қазақстан Республикасындағы қорғаудың заңнамалық шаралары.\*Ақпараттандыру туралы Қазақстан Республикасының Заңы\*Қазақстан Республикасының Мемлекеттік құпиялар туралы заңы\*Қазақстан Республикасының Байланыс туралы Заңы.(Формасы: Аннотация жазу) | ОН 1 | ЖК 1.3 |  | 10 | IT 2 | office hours |
| Сенбі 23.00 - ТК 6, СӨЖ 2тапсырудың мерзімі |
| 7 | **Д.7.** Ашық кілттерді шифрлау жүйелерін құру принципі | ОН 2 | ЖК 2.2 | 1 |  |  | дәріс |
| **ПС.7.** RSA Ашық кілтті ақпараттық қауіпсіздік алгоритмі | ОН 2 | ЖК 2.2 | 1 | 20 | TK 7 | Workshop. |
| Сенбі 23.00 - ТК 7тапсырудың мерзімі |
| 8 | **Д.8.** Хэш функциялары | ОН 2 | ЖК 2.2 | 1 |  |  | дәріс |
| **ПС.8.** Цифрлық қолтаңба алгоритмдері. | ОН 2 | ЖК 2.2 | 1 | 10 | TK 8 | Workshop. |
|  |  |  |  |  |  |  |
| **СРСП 3** СӨЖ3 бойынша консультация |  |  |  |  |  | office hours |
| **СӨЖ** **3.** Қауіпсіздік сертификаттары. Қауіпсіздік сертификаттарының түрлері. | LO 3 | ЖК 3.1 |  | 15 | IT 3 | office hours |
| Сенбі 23.00 - ТК 8, СӨЖ 3тапсырудың мерзімі |
| 9 | **Д.9.** Арна деңгейінде желілерді сегменттеу. Ішкі желілерді жасау үшін VLAN технологиясын пайдалану. VLAN желісін пайдаланатын типтік желі топологиясы. | ОН 2 | ЖК 2.1ЖК 2.2ЖК 2.3 | 1 |  |  | дәріс |
| **ПС.9.** Цифрлық қолтаңба алгоритмдері. | ОН 2 | ЖК 2.1ЖК 2.2 | 1 | 15 | TK 9 | Workshop  |
|  |  |  |  |  |  |  |
| Сенбі 23.00 - ТК 9тапсырудың мерзімі |
| 10 | **Д.10.** Портқа негізделген VLAN желілері | ОН 2 | ЖК 2.3 | 1 |  |  | дәріс |
| **ПС.10.** IEEE 802.1 Стандарт | ОН 2 | ЖК 2.2ЖК 2.3 | 1 | 20 | TK 10 | Workshop  |
| Сенбі 23.00 - ТК 10тапсырудың мерзімі |
| **МТ (Midterm Exam)** |  |  |  | **100** |  |  |
| 11 | **Д.11.** Брандмауэр технологиялары. Желілік технологиялардың негізгі түсініктері (протоколдар стегі, TCP қосылу күйлері). Брандмауэр классификациясы | ОН 2 | ЖК 2.3 | 1 |  |  | дәріс |
| **ПС.11.** Брандмауэрді басқару негіздері. | ОН 2 | ЖК 2.3 | 1 | 18 | TK 11 | Workshop  |
| **СРСП 4** СӨЖ4 бойынша консультация |  |  |  |  |  | office hours |
| **СӨЖ** 4**.** Case Study. Байланыс деңгейінің протоколдары. L2TP протоколы бойынша екі жергілікті желіні қосу. | ОН 3 | ЖК 3.1 |  | 10 | IT 3 | office hours |
| Сенбі 23.00 - ТК 11, СӨЖ 4тапсырудың мерзімі |
|  |
| 12 | **Д.12**. Туннельдік технологиялар. Байланыс деңгейінің протоколдары. IPSec протоколдар тобы. | ОН 3 | ЖК 3.1ЖК 3.2 | 1 |  |  | дәріс |
| **ПС.12.** Протокол GRE | ОН 3 | ЖК 3.1 | 1 | 17 | TK 12 | Workshop  |
| Сенбі 23.00 - ТК 12 тапсырудың мерзімі |
| 13 | Д.13. Протокол SSL/TLS. | ОН 4 | ЖК 4.1ID 4.2 | 1 |  |  | дәріс |
| ПС.13. SIEM: IBM QRadar, McAfee ESM, Cisco MARS жүйелерді талдау | ОН 4 | ЖК 4.1 | 1 | 15 | TK 13 | Workshop  |
|  |  |  |  |  |  |  |
| **СРСП** 5 СӨЖ5 бойынша консультация |  |  |  |  |  | office hours |
| **СӨЖ** 5 Case StudyТақырып Symmetric DES шифрлау алгоритмі. | ОН 4 | ЖК 4.2 |  | 25 | IT 5 | office hours |
| Сенбі 23.00 - ТК 13, СӨЖ 5тапсырудың мерзімі |
| 14 | **Д.14.** Интрузияны анықтау және алдын алу жүйелері (IDPS). IDPS негізгі мақсаты. IDPS жіктеу әдістері | ОН 5 | ЖК 5.1ЖК 5.2 | 1 |  |  | дәріс |
| ПС.14. Интрузияны анықтау және алдын алу жүйелері (IDPS).Вирусқа қарсы сканерлеу. | ОН 4 | ЖК 5.1 | 1 | 10 | TK 14 | Workshop  |
| Сенбі 23.00 - ТК 14 тапсырудың мерзімі |
| 15 | **Д.15**. Қозғалыс басымдылығы және балама бағыттарды құру. Интернетке қол жеткізудің баламалы бағыттарын құру | ОН 5 | ЖК 5.1ЖК 5.2 | 1 |  |  | дәріс |
| **ПС.15.** IDP көмегімен трафикті қалыптастыру | ОН 5 | ЖК 5.2 | 1 | 10 | TK 15 | Workshop  |
| **СРСП 6** СӨЖ6 бойынша консультация |  |  |  |  |  | office hours |
| **СӨЖ 6** Осалдықтардың деректер базасы. | ОН 5 | ЖК 5.1ЖК 5.2 |  | 25 | IT 6 | office hours |
| Жұма 23.00 - ТК 15, СӨЖ 15тапсырудың мерзімі |
| **CW 2** |  |  |  | **100** |  |  |

Қатты дене физикасы және бейсызық физика кафедрасының мәжілісінде қаралды және ұсынылды «\_\_» 2022 ж., хаттама №

Кафедра меңгерушісі М.К. Ибраимов

Факультеттің әдістемелік бюросының отырысында бекітілді

"\_\_" \_\_\_\_ 2022 ж., №\_\_ хаттама

Факультеттің әдістемелік бюросының төрағасы Р. Машеева

Бағдарлама факультеттің Ғылыми кеңесінде бекітілді.

"\_\_" \_\_\_\_ 2020 ж., №\_\_ хаттама

Ғылыми кеңестің төрағасы,

факультет деканыA.Е. Давлетов

Лектор A.K. Иманбаева