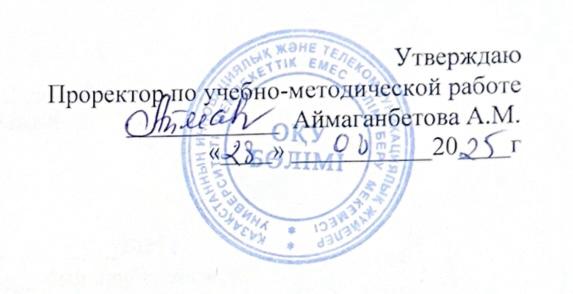
****

**КАЗАХСТАНСКИЙ УНИВЕРСИТЕТ ИННОВАЦИОННЫХ И  
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ**



**Программа обучения по дисциплине (силлабус)**

**Методы и средства защиты компьюерной информации**

**(***название дисциплины***)**

**для обучающихся пообразовательной программе**

**6В06114-«Вычислительная техника и программное обеспечение»**

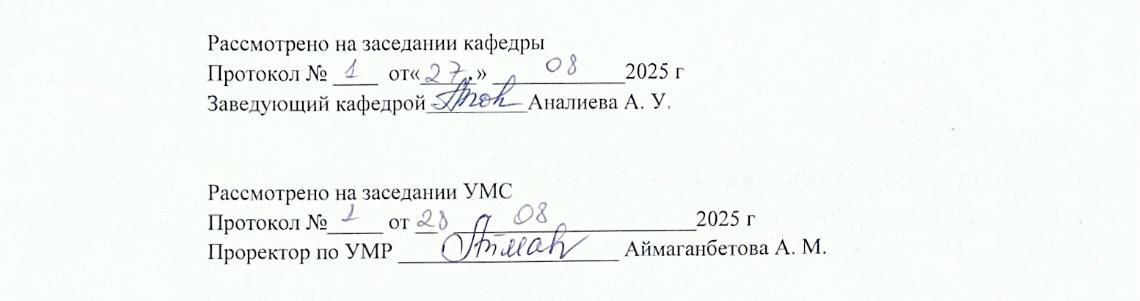
*(код и название ОП)*

г. Уральск 2025 год

Разработчик:

*ФИО* Курмашева Лайла Жубандыковна

*Академическая степень* ст. препод., м.т.н.



1. **Календарно-тематический план по теме «**Методы и средства защиты компьютерной информации**».**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ап** | **Модуль и тема** | **Лекции** | **Практика** | **СРОП** | **СРО** | **Итого** |
|  |  |
| **слишком** | **имя** |  |  |  |
|  |  |
|  |  |  |  |  |  |

**Модуль 1. Теоретические и практические методы защиты информации.**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. | | Введение. | | Курс | | | | | | | | цель и | | | | | | | | |  | |  | |  | |  | |  | |
|  | | задачи, в процессе его изучения | | | | | | | | | | | | | | | | | | | 1 | |  | |  | |  | |  | |
|  | | место, которое нужно занять. Защита информации | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |
|  | |  | |  | |  | |  | |  | |
|  | | классификация инструментов. | | | | | | | | | | | |  | | | | |  | |  | |  | |  | |  | |  | |
|  | | Без разрешения | | | | | | | от копирования | | | | | | | | | | защита | |  | | 2 | |  | | 5 | | 9 | |
|  | | знакомство с методами. | | | | | | | | | | | |  | | | | |  | |  | |  | |
|  | |  | | | | |  | |  | |  | |  | |  | |  | |
|  | | Текущий | | информативный | | | | | | | | | | в процессе | | | | | | |  | |  | |  | |  | |  | |
|  | | информации | | | | | | | безопасность | | | | | | | | | | я | |  | |  | | 1 | |  | |  | |
|  | | защита | | система | | | | | | | | могу получить | | | | | | | место | |  | |  | |  | |  | |
|  | |  | |  | |  | |  | |  | |
|  | | и роль. | | | | | | |  | | |  | |  | | | | |  | |  | |  | |  | |  | |  | |
| 2. | | Информационный | | | | | | |  | | |  | | в процессах | | | | | | |  | |  | |  | |  | |  | |
|  | | введите информацию, | | | | | | | | | | проблема | | | | | | | | | 1 | |  | |  | |  | |  | |
|  | | обработка | | и | | | | | сохранить | | | | | | | | | | осуществленный | |  | |  | |  | |  | |
|  | |  | |  | |  | |  | |  | |
|  | | защита информации при внедрении | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | | Методы шифрования. | | | | | | | | | |  | |  | | | | |  | |  | | 2 | |  | | 5 | | 9 | |
|  | | Простые шифры | | | | | | | | | | | |  | | | | |  | |  | |  | |
|  | |  | | | | |  | |  | |  | |  | |  | |  | |
|  | |  | | | | | | |  | | | | |  | | | | | | |  | |  | |  | |  | |  | |
|  | | Информация | | | | | | | защита | | | | | отчеты | | | | | | |  | |  | |  | |  | |  | |
|  | | решать. | |  | | | | | В криптографии | | | | | | | | | | | |  | |  | | 1 | |  | |  | |
|  | | модульный | | | | | | | арифметики | | | | | | | | | | | |  | |  | |  | |  | |
|  | |  | |  | |  | |  | |  | |
|  | | использовать | | | | | | |  | | |  | |  | | | | |  | |  | |  | |  | |  | |  | |
| 3. | | Методы защиты информации и | | | | | | | | | | | | | | | | | | | 1 | |  | |  | |  | |  | |
|  | | инструменты. | | | | | | |  | | |  | |  | | | | |  | |  | |  | |  | |  | |
|  | |  | | |  | |  | | | | |  | |  | |  | |  | |  | |  | |
|  | | Псевдослучайный | | | | | | | | | |  | | цепи | | | | | | |  | | 2 | |  | |  | |  | |
|  | | методы генерации. | | | | | | | | | | | | | | | | |  | |  | |  | | 5 | | 9 | |
|  | |  | |  | |  | |  | |
|  | |  | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | | Свойства конечных полей и | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | | криптография. | | | | | | | | | | Шифрование | | | | | | | | |  | |  | | 1 | |  | |  | |
|  | | изучение классических систем | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
| 4. | | Теоретическая защита информации | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | | методы. | | | | | | | Псевдослучайный | | | | | | | | | | | | 1 | |  | |  | |  | |  | |
|  | | методы генерации схем | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | | Текущий | | когда | | | | | | | | использовал | | | | | | | | |  | |  | |  | | 5 | | 9 | |
|  | | оперативный | | | | | | | содержится в среде | | | | | | | | | | | |  | |  | |  | |
|  | |  | |  | |  | |  | |  | |
|  | | криптографический | | | | | | | | | |  | |  | | | | |  | |  | | 2 | |  | |  | |  | |
|  | |  | |  | | | | |  | |  | |  | |  | |  | |
|  | | функций | | | | | | | | | |  | | с работой | | | | | | |  | |  | |  | |  | |  | |
|  | | знакомство | |  | | | | |  | | |  | |  | | | | |  | |  | |  | |  | |  | |  | |
|  | | Идентификация | | | | | | | |  | | | |  |  | | | | и | |  | |  | |  | |  | |  | |
|  | | аутентификация | | | | | | | | процедуры. | | | | | | | | | | |  | |  | | 1 | |  | |  | |
|  | | Шифрование | | | | | | | | симметричный | | | | | | | | | | |  | |  | |  | |  | |
|  | |  | |  | |  | |  | |  | |
|  | | изучение несистем | | | | | | | | | | | | |  | | | |  | |  | |  | |  | |  | |  | |
|  | | **Модуль 2. Программные средства защиты информации** | | | | | | | | | | | | | | | | | | | | | | | | | | |  | |
|  | |  | | | | |  | | |  | | | |  | | | | | | |  | |  | |  | |  | |  | |
| 5. | | Информация | | | | |  | | |  | | | | защиты | | | | | | | 1 | |  | |  | |  | |  | |
|  | | экспериментальные методы. | | | | | | | | | | | |  |  | | | |  | |  | |  | |  | |  | |
|  | |  |  | | | |  | |  | |  | |  | |  | |  | |
|  | | Традиционные методы шифрования. | | | | | | | | | | | | | | | | | | |  | | 2 | |  | |  | |  | |
|  | |  | | | | | | | | | | | |  |  | | | | | |  | |  | |  | |  | |  | |
|  | | информации ИБ | | | | | | | | | | | |  | целостность | | | | | |  | |  | |  | | 5 | | 9 | |
|  | | предоставлять | | | | | делать | | | | | | | | контроль | | | | | |  | |  | |  | |
|  | | сумма | | | | | метод | | | | | | |  | использовать. | | | | | |  | |  | | 1 | |  | |  | |
|  | | Защита | | |  | |  | | |  | | | | оптимальный | | | | | | |  | |  | |  | |  | |
|  | |  | |  | | |  | | | |  | |  | |  | |  | |  | |
|  | | управления | | | | |  | | |  | | | | моделирование | | | | | | |  | |  | |  | |  | |  | |
|  | | программы обработки | | | | | | | | | | | | |  | | | |  | |  | |  | |  | |  | |  | |
| 6. | | Компьютеры | | | | | | | | я | | | | в сетях | | | | | | |  | |  | |  | |  | |  | |
|  | | информация | | | | |  | | |  | | | | защиты | | | | | | | 1 | |  | |  | |  | |  | |
|  | | программные инструменты. | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |  | |
|  | | Потоковые шифры. | | | | | | | | | | | |  |  | | | |  | |  | | 2 | |  | |  | |  | |
|  | | Открыть | | | ключ | | | | | криптография. | | | | | | | | | | |  | |  | |  | | 5 | | 9 | |
|  | | Необходимый | | | алгоритмы | | | | | | | | | | | | | | читать | |  | |  | |  | |
|  | | учиться | | |  | | и | | | | | | | теоретически | | | | | | |  | |  | |  | |  | |  | |
|  | | подробности. | | | | |  | | |  | | | |  | Окна | | | | | |  | |  | | 1 | |  | |  | |
|  | | оперативный | | | | | | | | система | | | | | на основе | | | | | |  | |  | |  | |  | |  | |
|  | | онлайн | | |  | | защита | | | | | | |  | сложный | | | | | |  | |  | |  | |  | |  | |
|  | | определить оценку | | | | | | | | | | | |  |  | | | |  | |  | |  | |  | |  | |  | |
| 7. | | Компьютеры | | | | | | | | я | | | | в сетях | | | | | | |  | |  | |  | |  | |  | |
|  | | информация | | | | | защита. | | | | | | | Информация | | | | | | | 1 | |  | |  | |  | |  | |
|  | | компьютер | | | | | | | |  | | | | от вирусов | | | | | | |  | |  | |  | |  | |
|  | |  | | | |  | |  | |  | |  | |  | |
|  | | защита. | | |  | |  | | |  | | | |  |  | | | |  | |  | |  | |  | |  | |  | |
|  | | Блокировать | | |  | | шифры. | | | | | | | | Работа | | | | | |  | | 2 | |  | | 5 | | 9 | |
|  | | режимы. | | | | |  | | |  | | | |  |  | | | |  | |  | |  | |
|  | |  | | |  | | | |  |  | | | |  | |  | |  | |  | |  | |  | |
|  | |  | | |  | | | | |  | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | | Открыть | | | ключ | | | | | криптография. | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | | Модуль | | | в соответствии с | | | | | | | | | весь | | | | | число | |  | |  | | 1 | |  | |  | |
|  | | степень | | | | | расчет | | | | | | | алгоритм. | | | | | | |  | |  | |  | |  | |
|  | |  | |  | |  | |  | |  | |
|  | | Использование методов шифрования | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
| 8. | | Программный | | | | | | | |  | | | | содержание | | | | | | |  | |  | |  | |  | |  | |
|  | |  | | | | 1 | |  | |  | |  | |  | |
|  | | защита от несанкционированного использования. | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | |  | | |  | |  | | |  | | | |  |  | | | |  | |  | |  | |  | | 5 | | 9 | |
|  | | Криптографические алгоритмы | | | | | | | | | | | | | | | | | | |  | |  | |  | |
|  | |  | | 2 | |  | |  | |  | |
|  | | использовать | | |  | | через | | | | | | | информация | | | | | | |  | |  | |  | |  | |
|  | |  | |  | |  | |  | |  | |  | |
|  | | шифрование. | | |  | |  | | |  | | | |  |  | | | |  | |  | |  | |  | |  | |  | |
|  | |  | | |  | |  | | |  | | | |  |  | | | |  | |  | |  | |  | |  | |  | |
|  | | Диффи-Хеллман | | | | | | | | | |  | | | | схема | | | | |  | |  | | 1 | |  | |  | |
|  | | в соответствии с | | | | ключи | | | | | | замена | | | | | | | | |  | |  | |  | |  | |
|  | |  | |  | |  | |  | |  | |
|  | | Средства антивирусной защиты | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | |  | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | | **Модуль 3. Криптографические инструменты** | | | | | | | | | | | | | | | | | | | | | | |  | |  | |  | |
| 9. | | Калькулятор | | | | к системам | | | | | | | | | | вовлеченный | | | | |  | |  | |  | |  | |  | |
|  | |  | |  | |  | |  | |  | |
|  | | ты опасен | | типы. Компьютер | | | | | | | | | | | | | | | | | 1 | |  | |  | |  | |  | |
|  | | в сетях | | | | | | | на расстоянии | | | | | | | атаковать | | | | |  | |  | |  | |  | |  | |
|  | | классификация и анализ | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | |  | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | | Криптографические алгоритмы | | | | | | | | | | | | | | | | | | |  | | 2 | |  | |  | |  | |
|  | | использовать | |  | | через | | | | | | информация | | | | | | | | |  | |  | | 5 | | 9 | |
|  | |  | |  | |  | |  | |
|  | | шифрование, дешифрование. | | | | | | | | | | | | | |  |  | | | |  | |  | |  | |
|  | |  |  | | | |  | |  | |  | |  | |  | |
|  | |  | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | | Криптография с открытым ключом. ЮАР | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | | открыть | | ключ | | | | | шифрование | | | | | | | | метод. | | | |  | |  | | 1 | |  | |  | |
|  | | Из дизассемблера | | | | | | | | | |  | | | |  | и | | | |  | |  | |  | |  | |
|  | |  | | | |  |  | |  | |  | |  | |  | |
|  | | от процессоров | | | | | | | | | |  | | | |  | защита | | | |  | |  | |  | |  | |  | |
|  | | процедуры обработки | | | | | | | | | | | | | |  |  | | | |  | |  | |  | |  | |  | |
|  | |  | |  | |  | | |  | | |  | | | |  |  | | | |  | |  | |  | |  | |  | |
| 10. | | Информация | | | | разрушитель | | | | | | от эффектов | | | | | | | | |  | |  | |  | |  | |  | |
|  | | 1 | |  | |  | |  | |  | |
|  | | программа защиты | | | | | | | | | | | | | |  |  | | | |  | |  | |  | |  | |  | |
|  | |  | | | | | | |  | | |  | | | | | | | | |  | |  | |  | |  | |  | |
|  | | Криптоанализ | | | | | | |  | | | элементы. | | | | | | | | |  | | 2 | |  | |  | |  | |
|  | | В тексте | | | |  | | | символов | | | | | | | | | | | |  | |  | |  | |  | |
|  | |  | | |  | |  | |  | | 5 | | 9 | |
|  | | оценка частоты. | | | | | | | | | |  | | | |  |  | | | |  | |  | |  | |
|  | |  | | | |  |  | | | |  | |  | |  | |  | |  | |
|  | |  | | | |  | | | | | |  | | | | | | | | |  | |  | |  | |  | |  | |
|  | | Шифрование | | | | методы | | | | | | использовать. | | | | | | | | |  | |  | |  | |  | |  | |
|  | | Защита | |  | |  | | | процедуры | | | | | | | | | | | |  | |  | | 1 | |  | |  | |
|  | | сложность | | | | | | | сложный | | | | | | |  | оценка | | | |  | |  | |  | |  | |  | |
|  | | и исследования | | | | | | |  | | |  | | | |  |  | | | |  | |  | |  | |  | |  | |
|  | |  | |  | |  | | |  | | |  | | | |  |  | | | |  | |  | |  | |  | |  | |
| 11. | | Информация | | | |  | | |  | | | защиты | | | | | | | | |  | |  | |  | |  | |  | |
|  | |  | | |  | | | 1 | |  | |  | |  | |  | |
|  | | криптографические инструменты. | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | |  | |  | |  | | |  | | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | | Смешанный | |  | |  | | | криптографический | | | | | | | | | | | |  | | 2 | |  | | 5 | | 9 | |
|  | | алгоритмы | | | | | | |  | | |  | | | |  |  | | | |  | |  | |  | |
|  | |  | | |  | | | |  |  | | | |  | |  | |  | |  | |  | |
|  | |  | |  | | | | | | | | | | | | |  | | | |  | |  | |  | |  | |  | |
|  | | Защита | | процедуры | | | | | | | | | | | | | обработка. | | | |  | |  | | 1 | |  | |  | |
|  | | Оптимизация процессов защиты | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |
|  | |  | |  | |  | |  | |  | |
|  | | создание моделей управления. | | | | | | | | | | | | | | | | | | |  | |  | |  | |  | |  | |
|  | |  | | | | | | | | | | | | | |  | | | | |  | |  | |  | |  | |  | |
| 12. | | Системы открытого типа. | | | | | | | | | | | | | | Цифровой | | | | | 1 | |  | |  | |  | |  | |
|  | | подпись | | | |  | | |  | | |  | | | |  |  | | | |  | |  | |  | |  | |
|  | |  | | |  | | |  | | | |  |  | | | |  | |  | |  | |  | |  | |
|  | | Асимметричный | | | | | | | | | |  | | | |  |  | | | |  | |  | |  | | 5 | | 9 | |
|  | | в криптосистемах | | | | | | | | | | подробности | | | | | | | | |  | | 2 | |  | |  | |  | |
|  | | методы шифрования. | | | | | | | | | |  | | | |  |  | | | |  | |  | |  | |  | |  | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Защита | процедуры | |  |  |  |  |  |
|  | сложность | изучать | и |  |  |  |  |  |
|  | сложный | оценка. | псевдо- |  |  | 1 |  |  |
|  | случайно | цифры | датчик |  |  |  |  |  |
|  | оценка качества | |  |  |  |  |  |  |

Модуль 4. Меры защиты информации. Оценка уровня безопасности

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. | Сеть | интервал | |  | экраны | 1 |  |  |  |  |
|  | технология. | | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  | Хэштег |  | алгоритм | | и |  |  |  |  |  |
|  | электронный | |  |  | цифровой |  | 2 |  |  |  |
|  | фирменная работа. | | |  |  |  |  |  |  |  |
|  |  | | |  |  |  |  |  | 5 | 9 |
|  | Программный | | |  |  |  |  |  |
|  | обеспечение | | | | защищать |  |  |  |  |  |
|  | с целью | | ключ | | дискета |  |  | 1 |  |  |
|  | подготовка. | |  | Пользователь | |  |  |  |  |
|  |  |  |  |  |  |  |
|  | идентификация | | |  | и |  |  |  |  |  |
|  | аутентификация | | |  |  |  |  |  |  |  |
| 14. | VPN | виртуальный | |  | защищенный |  |  |  |  |  |
|  | сетей | |  |  | основной | 1 |  |  |  |  |
|  | технологии. | | |  |  |  |  |  |  |  |
|  | Электронно-цифровая подпись | | | | |  | 2 |  |  |  |
|  |  | | |  |  |  |  |  | 5 | 9 |
|  | Псевдослучайный | | |  | цифры |  |  |  |
|  | датчики | | качество | | оценка. |  |  |  |  |  |
|  | Операционная среда | | | содержит | |  |  | 1 |  |  |
|  | реализованный криптографический | | | | |  |  |  |  |  |
|  | функции обучения | | | |  |  |  |  |  |  |
| 15. | Виртуальный | |  |  | защищенный |  |  |  |  |  |
|  | каналы | | создавать | версии. | | 1 |  |  |  |  |
|  | VPN-безопасность | | | предоставлять | |  |  |  |  |
|  |  |  |  |  |  |
|  | методы изготовления | |  |  |  |  |  |  | 5 | 9 |
|  | С вирусами | |  |  | борьба |  | 2 |  |
|  |  |  |  |  |  |  |
|  | Антивирусные программы. | | | | |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |  |
|  | Различный | шифрование | |  | методы |  |  | 1 |  |  |
|  | провести сравнительный анализ. | | | | |  |  |  |  |
|  |  |  |  |  |  |
|  |  | **Все** | |  |  | **15** | **30** | **45** | **60** | **150** |

1. **Академическая политика курса**

****

опоздание на урок;

Пропуск занятий, предъявление медицинской справки при болезни; Сдавать уроки в указанное преподавателем время; Тщательное и внимательное выполнение отдельных задач; Приходить на занятие одетым согласно внутренним требованиям университета; Не жуйте жвачку во время занятий;



Выключите мобильный телефон;



Не срывайте урок.

Время консультаций: понедельник-пятница с 15:00 до 16:30.

1. **График задач CSIRO**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Нет** | **Модуль и** | | | | **Задачи** | **Литература** | **Отчетность** |  | **Задача** |
|  | **представить** |
| **р/р** | **название темы** | | | |  | **(Нет.)** | **форма** |  |
|  |  | **время, неделя** |
|  |  |  |  |  |  |  |  |  |
|  | **Модуль 1. Теоретические и практические методы защиты информации.** | | | | | | | | |
|  |  |  |  | |  |  |  |  |  |
|  | Текущий |  | информативный | | Информация | Основной: |  |  |  |
|  | в процессе | | информации | |  |  |  |
|  | безопасность. | 1,2,6 | Теоретический |  |  |
| 1 | безопасность | | я | защита |  | Неделя 1 |
| Информация | Дополнительный: | запрос |  |
|  | расположение системы, | | | |  |  |
|  | система защиты. | 13 |  |  |  |
|  | роль. |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | В криптографии | | | | Модульность | Основной: |  |  |  |
| 2 | модульный | |  |  | арифметика | 1,2,6 | глоссарий |  | 2-я неделя |
| арифметики | | |  | использовать | Дополнительный: |  |
|  |  |  |  |  |
|  | использовать | |  |  | примеры | 14 |  |  |  |
|  | Бесконечный | |  | поля |  | Основной: |  |  |  |
|  |  | Характеристики | 3-5 | отчеты |  |  |
| 3 | характеристики | |  | и |  | Неделя 3 |
|  | использовать | Дополнительный: | выпускать |  |
|  | криптография | | |  |  |  |
|  |  |  | 13 |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | Идентификация | | | и |  | Основной: |  |  |  |
|  | Процедуры | 3-5 | отчеты |  |  |
| 4 | аутентификация | | |  |  | 4-я неделя |
|  | использовать | Дополнительный: | выпускать |  |
|  | процедуры | | |  |  |  |
|  |  |  | 13 |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  | **Модуль 2. Программные средства защиты информации** | | | | | | |  |
|  |  |  | | |  |  |  |  |  |
|  | ЯВЛЯЕТСЯ | информация | | |  | Основной: |  |  |  |
|  | целостность | | предоставлять | | Контроль |  |  |  |
|  | 3-5 | отчеты |  |  |
| 5 | делать | для | контроль | | дополнения |  | Неделя 5 |
| Дополнительный: | выпускать |  |
|  | сумма | |  | метод | метод расчета |  |  |
|  |  | 14 |  |  |  |
|  | использовать | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  | Открыть |  |  | ключ | Евклид | Основной: |  |  |  |
|  | криптография. Необходимый | | | | алгоритм. |  |  |  |
|  | 2,3,5 | отчеты |  |  |
| 6 | алгоритмы | | | читать | В степени |  | Неделя 6 |
| Дополнительный: | выпускать |  |
|  | учебный и теоретический | | | | быстрый выпуск |  |  |
|  | 14 |  |  |  |
|  | подробности | |  |  | алгоритм. |  |  |  |
|  |  |  |  |  |  |  |
|  | Открыть |  |  | ключ | Степени | Основной: |  |  |  |
|  | криптография. | | | Модуль |  |  |  |
|  | расчет | 2, 4 | Программа |  |  |
| 7 | в соответствии с | | целое число | |  | 7-я неделя |
| алгоритм, | Дополнительный: | листинг |  |
|  | степень | |  | расчет |  |  |
|  |  | генерировать | 15 |  |  |  |
|  | алгоритм. | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  | Диффи-Хеллман | | | | С ключами | Основной: |  |  |  |
|  | 3, 5 | Программа |  |  |
| 8 | схема | | в соответствии с | | обмен |  | Неделя 8 |
| Дополнительный: | листинг |  |
|  | обмен ключами | | | | алгоритм |  |  |
|  | 16 |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  | **Модуль 3. Криптографические инструменты** | | | | |  |
|  |  |  |  |  |  |  |  | |  |
| 9 | Открыть |  |  | ключ | RSA — открытый ключ | Основной: | Расчеты |  | 9-я неделя |
|  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | криптография. | | ЮАР | метод шифрования. | 3, 5 | выпускать |  |
|  | открыть | ключ | шифрование |  | Дополнительный: |  |  |
|  | метод. |  |  |  | 16 |  |  |
|  |  |  |  | Блокировать |  |  |  |
|  |  |  |  | шифрование | Основной: |  |  |
| 10 | Шифрование | | методы | стандарты. | 1,2,6 | абстрактный | 10-я неделя |
| использовать | |  | Один ключ | Дополнительный: |
|  |  |  |  |
|  |  |  |  | шифры. | 15 |  |  |
|  |  |  |  | Шифр Блоуфиша. |  |  |  |
|  |  |  |  | Защищенная ОС- | Основной: |  |  |
| 11 | Защита |  |  | создать | 6-10 | Теоретический | 11-я неделя |
| процедуры обработки | | | иерархический | Дополнительный: | запрос |
|  |  |
|  |  |  |  | используя метод | 16 |  |  |
|  | Защита | процедуры | | Честность | Основной: |  |  |
|  | 6-10 | Расчеты |  |
| 12 | контроль | 12-я неделя |
| сложность | | изучать | Дополнительный: | выпускать |
|  | политическая модель |  |
|  | и комплексная оценка | | | 15 |  |  |
|  |  |  |  |
|  |  | | |  |  |  |  |
|  | **Модуль 4. Меры защиты информации. Оценка уровня безопасности** | | | | | | |
|  |  |  |  |  |  |  |  |
|  |  |  |  | Защита |  |  |  |
|  |  |  |  | организатор |  |  |  |
|  |  |  |  | меры |  |  |  |
|  | Программный | | | во время проектирования | Основной: |  |  |
|  | обеспечение | | | безопасность |  |  |
|  | 6-10 | Теоретический |  |
| 13 | защищать | с целью | | предоставлять | Неделя 13 |
| Дополнительный: | запрос |
|  | ключ |  | дискета | процессы |  |
|  |  | 14 |  |  |
|  | подготовка | |  | оптимальный |  |  |
|  |  |  |  |  |
|  |  |  |  | управление |  |  |  |
|  |  |  |  | модели, |  |  |  |
|  |  |  |  | методы |  |  |  |
|  |  |  |  | Программный |  |  |  |
|  | Псевдослучайный | | | продукты | Основной: |  |  |
|  | тестирование | 6-10 | Расчеты |  |
| 14 | цифры | датчики | | 14 недель |
| проблемы, | Дополнительный: | выпускать |
|  | оценка качества | | |  |
|  | автоматически | 15 |  |  |
|  |  |  |  |  |  |
|  |  |  |  | тестирование |  |  |  |
|  | Различный | | шифрование | Шифрование | Основной: |  |  |
|  | методы |  |  |
|  | методы | |  | 6-10 |  |  |
| 15 |  | статистический | коллоквиум | 15 недель |
| родственник | | анализ | Дополнительный: |
|  | характеристики |  |  |
|  | вождение | |  | 16 |  |  |
|  |  | изучать |  |  |
|  |  |  |  |  |  |  |

1. **Критерии оценки знаний по предмету и график выполнения заданий**

Таблица 1. Текущая оценка прогресса

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | |  | | Виды уроков | | | |  | |
|  | Неделя | | Практичный | | | | БАСФ | |  | |
|  | номер задачи | | счет | | Номер задачи |  | счет | |
|  |  | |  |
|  |  | |  | |  | |  |  |  | |
| 1 |  | | 2 | | 2\*100 | | 4 |  | 4\*100 | |
| 2 |  | | 2 | | 2\*100 | | 4 |  | 4\*100 | |
| 3 | | | 2 | | 2\*100 | | 4 | | 4\*100 | |
| 1 РБ средний балл | | |  | | 1 СБ = ((600+1200)/18+100)/2 =100 | | | |  | |
| 4 | | | 2 | | 2\*100 | | 4 | | 4\*100 | |
| 5 | | | 2 | | 2\*100 | | 4 | | 4\*100 | |
| 6 | | | 2 | | 2\*100 | | 4 | | 4\*100 | |
| 2 РБ средний балл | | |  | | 2 СБ = ((600+1200)/18+100)/2 =100 | | | |  | |
| 7 | | | 2 | | 2\*100 | | 4 | | 4\*100 | |
| 8 | | | 2 | | 2\*100 | | 4 | | 4\*100 | |
| 9 | | | 2 | | 2\*100 | | 4 | | 4\*100 | |
| 3 РБ средний балл | | |  | | 3 СБ = ((600+1200)/18+100)/2 =100 | | | |  | |
| 10 | | | 2 | | 2\*100 | | 4 | | 4\*100 | |
| 11 | | | 2 | | 2\*100 | | 4 | | 4\*100 | |
| 12 | | | 2 | | 2\*100 | | 4 | | 4\*100 | |
| 4 РБ средний балл | | |  | | 4 СБ = ((600+1200)/18+100)/2 =100 | | | |  | |
| 13 | | | 2 | | 2\*100 | | 4 | | 4\*100 | |
| 14 | | | 2 | | 2\*100 | | 4 | | 4\*100 | |
| 15 | | | 2 | | 2\*100 | | 4 | | 4\*100 | |
| 5 РБ средний балл | | |  | | 5 СБ = ((600+1200)/18+100)/2 =100 | | | |  | |

**Рейтинг проходного балла**рассчитывается как среднее арифметическое суммы пяти оценок и рассчитывается в процентах следующим образом:

РБ1 + РБ2 + РБ3 + РБ4 + РБ5

Рор =

5

Здесь: Ror – среднее значение рейтингового балла;

РБ 1/2/3/4/5 – 1-й, 2-й, 3-й, 4-й, 5-й по рангу контроль соответственно.

**Итоговый контроль (экзамен)**оно проводится в форме письменного, устного, тестирования и комплексного опроса.

Форма и порядок проведения экзамена по каждому учебному предмету определяются решением Ученого совета университета за один месяц до начала учебного периода.

В форме тестирования возможно проведение комплексного экзамена по двум и более предметам, но здесь эти предметы должны быть профессионально направленными или родственными.

На выпускной экзамен направляются студенты, не имеющие академической задолженности по обязательным предметам и набравшие более 50% среднего значения рейтингового балла.

Итоговая оценка рассчитывается только в случае получения студентом положительной оценки на рейтинговом проходе (50% и выше рейтингового балла), а также на итоговом контроле (50% и выше итогового балла).

Текущий контроль успеваемости составляет 70% итоговой оценки знаний по предмету, а оценка ЕГЭ составляет 30% итоговой оценки по предмету.

ПБ\* = Рор х 0,7 + ПБ х 0,3

где: PB\* — итоговая оценка

Ror – среднее значение рейтингового контроля;

ПА – финальный контроль

Преподаватель вносит результаты экзамена в протокол экзамена в день экзамена.

Если обучающийся не согласен с результатом рейтинговой оценки и/или итогового контроля, обучающийся имеет право подать апелляцию в течение одного дня с даты проведения рейтинговой оценки и/или экзамена. После каждой оценки, если обучающийся согласен с оценкой, он подписывает графу «Знакомство» рейтингового листа, и это считается основанием для отказа в апелляции.

Для повторной подачи положительной оценки итогового контроля (в целях продвижения по службе) обучающийся перечитывает все виды занятий, указанные в учебной программе по данному предмету, получает квалификационный допуск и сдает итоговый контроль. Пересдача итоговой проверки с «неудовлетворительной» оценки на положительную осуществляется в таком порядке.

В качестве средства измерения знаний учащихся вводится шкала оценок.

Шкала оценок основана на балльно-рейтинговой буквенной системе.

Оценка представляет собой оценочную шкалу, основанную на рейтинговой системе.

|  |  |  |  |
| --- | --- | --- | --- |
| **Алфавитная система** | **счет** | **Процент** | **ценить** |
| **цена на** | **количество, %** |
|  |  |
|  |  |  |  |
| А | 4.00 | 95-100 | Очень хороший |
|  |  |  |
| А- | 3,67 | 90-94 |
|  |
|  |  |  |  |
| B+ | 3.33 | 85-89 |  |
|  |  |  |  |
| В | 3.0 | 80-84 | Хороший |
|  |  |  |
| Б- | 2,67 | 75-79 |
|  |
|  |  |  |  |
| С+ | 2.33 | 70-74 |  |
|  |  |  |  |
| С | 2.0 | 65-69 |  |
|  |  |  |  |
| С- | 1,67 | 60-64 | Удовлетворение |
|  |  |  |
| Д+ | 1.33 | 55-59 |
|  |
|  |  |  |  |
| Д- | 1.0 | 50-54 |  |
|  |  |  |  |
| Форекс | 0,5 | 25-49 | Неудовлетворительный |
|  |  |  |
| Ф | 0 | 0-24 |
|  |
|  |  |  |  |

1. **Рекомендуемый список чтения:**

**Основная литература:**

* 1. Информационная безопасность и защита информации [Текст] : учебное пособие / Г. А. Камалова, Л. Б. Диярова. - Урал: БКАТУ имени Жангир хана, 2018. - 115 (7,2 стр.)

л.) с.

* 1. Кибербезопасность. Ч. Я. : учебное пособие / У. Б. Асылбеков, А. А. Исмаилова. – Алматы: «Бастау», 2019. – 360 с.
  2. Кибербезопасность. Часть II Кибербезопасность. Ч. II. : учебное пособие / У. Б. Асылбеков, А. А. Исмаилова. – Алматы: «Бастау», 2019. – 256 с.
  3. Баранова Е.К., Бабаш А.В. / Информационная безопасность и защита информации, РИОР, Инфра-М, 2017, 324 с.
  4. Нестеров С./ Основы информационной безопасности. Учебное пособие / Лан-Петербург, 2009. – 324 с.
  5. Нестеренко А., Рожков М./ Криптографические методы защиты информации. Учебник, М.: КноРус, 2016. – 192 с.
  6. Фомичев В., Мельников Д./ Криптографические методы защиты информации. Ч. 1 и 2., Издательство Юрайт, 2017. – 454 с.
  7. Партыка Т.Л., Попов И.И., Емельянова Н.З./ Защита информации в персональном компьютере, ФОРУМ, 2010. – 368 с.
  8. Платонов В.В./ Программно-аппаратная защита информации, Издательский центр «Академия», 2013. – 336 с.
  9. Мельников В.П., Клейменов С.А., Петраков А.М. / Информационная безопасность и защита информации, Издательский центр «Академия», 2012. – 336 с.
  10. Зайцев А., Мещеряков Р./ Технические средства и методы защиты информации. 7-е изд., Горячая линия-Телеком, 2012. - 442 с.
  11. Аяджанов К.С., Есенова А.С. Информационная безопасность и защита информации: Учеб. Алматы: ТОО РПБК «Давир», 2011. – 376 с.
  12. Ярочкин В.И./ Информационная безопасность: Учебник для студентов вузов, Академический проект, 2010. – 544 с.
  13. Проскурин В.Г. Защита программ и данных: учеб. пособие на учебу. университет
* бакалавриат / В. Г. Проскурин. - М. : Издательский центр «Академия», 2011. – 208 с.
  1. Форузан Б.А. Криптография и сети безопасности: учеб. пособие для студентов и аспирантов / Б. А. Форузан; пер. с англ. А. Н. Берлин. - М.: Интернет-университет информационных технологий; БИНОМ. Лаборатория знаний, 2010. – 784 с.
  2. Информационная безопасность в телекоммуникационных системах [Текст]: учебное пособие / Б. М. Якубов, А. К. Мекебаева. – Алматы: Альманах, 2017. – 75 с.

**Дополнительная литература:**

1. Адаменко М./ Основы классической криптологии. Тайна шифров и кодов,

ДМК-Пресс, 2012. – 256 с.

1. Климентьев К./ Компьютерные вирусы и антивирусы: взгляд программиста,

ДМК-Пресс, 2013. 656 с.

1. Левин М./ПГП: Кодирование и шифрование информации открытым ключом, Книга-Пресс, 2010. – 166 с.Шангин В./ Информационная безопасность компьютерных систем и сетей,

Инфра-М, 2011. – 416 с.

1. 5В070300-Методические указания к выполнению лабораторной работы по предмету «Информационная безопасность и защита информации» по специальности «Информационные системы» [Текст] / соавтор: Г. А. Камалова, А. Х. Давлетова, Т. М. Габшакирова. – Урал: БКАТУ имени Жангир хана, 2013. – 60 с.
2. Введение в защиту и безопасность информации: 051002 – по специальности «Системы информационной безопасности». / Комп. А.А. Шайкулова, Х.И. Юбузова. – Алматы: КазНТУ, 2009. – 96 с.
3. Методы и средства защиты информации: 5В070400 – по специальности «Вычислительная техника и программное обеспечение». / Комп. ГБ Кашаганова. – Алматы: КазНТУ, 2011. – 100 с.
4. Абдикалыков, К.А. Основы криптографии: Учеб. / Ассоциация высших учебных заведений Республики Казахстан. – Алматы: Полиграфкомбинат, 2012. – 184 с.