**СИЛЛАБУС**

**Весенний семестр 2020-2021 уч. год**

**по образовательной программе «Криптография и криптоанализ 2»**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Код дисциплины** | **Название дисциплины** | **Самостоятельная работа студента (СРС)** | **Кол-во часов** | | | | | **Кол-во кредитов** | | **Самостоятельная работа студента под руководством преподавателя (СРСП)** |
| **Лекции (Л)** | | **Практ. занятия (ПЗ)** | **Лаб. занятия (ЛЗ)** | |
| **KK3224** | **Криптография и криптоанализ 2** | 5 | 15 | | 15 | 30 | | 3 | | 37,6 |
| **Академическая информация о курсе** | | | | | | | | | | |
| Вид обучения | Тип/характер курса | Тип лекции | | Типы практических занятий | | | Кол-во **СРС** | | Форма итогового контроля | |
| On-лайн /  объединенная | теоретический | Проблемая, аналитическая | | Решение практических задач, криптографии и криптоанализа | | | Не менее 3-х | | Выполнение проекта | |
| Лектор | Бегимбаева Енлик Ериковна | | | | | | **Оф./с.** | | По расписанию  Подключиться к конференции Zoom  https://us04web.zoom.us/j/8506270133?pwd=bENGWlhXMDZyYTdHYWJkbWV1V2h6UT09  Идентификатор конференции:  850 627 0133  Код доступа: 2ZapZP | |
| **e-mail** | Enlik\_89@mail.ru | | | | | |
| **Телефон** | +77051000777 | | | | | |  | |  | |

|  |
| --- |
| **Академическая презентация курса** |

|  |  |  |
| --- | --- | --- |
| **Цель дисциплины** | **Ожидаемые результаты обучения (РО)**  В результате изучения дисциплины обучающийся будет способен: | **Индикаторы достижения РО (ИД)**  (на каждый РО не менее 2-х индикаторов) |
| **Целью освоения дисциплины «Криптография и криптоанализ 2 » является**  **обучение теоретическим и практическим знаниям, необходимым для решения широкого спектра**  **задач в области теоретической и прикладной криптографии и криптоанализа, с использованием**  **вероятностных и алгебраических моделей криптосистем, включающее знания основных**  **криптографических алгоритмов, способов построения криптографически стойких компонентов**  **шифров, а также математических методов, применяемых в криптоанализе блочных и поточных**  **шифров.** | **РО 1** (когнитивный) способность системного представления и понимания специфики научного знания и методологии исследования в рамках криптографических методов защиты информации; | **1.1**- интерпретировать понятия криптографии;  **1.2**- анализировать методы защиты информации. |
| **РО2** (функциональный) способность применять научные знания и знание методологии исследования в практике анализа материала в контексте современных научных криптографических методов защиты информации; сформировать способность к критическому анализу, оценке и синтезу новых идей в контексте криптографических методов защиты информации; | **2.1** – интерпретировать понятия защиты информации;  **2.2** –уметь вычилять по заданным алгоритмам шифрования и дешифрования. |
| **РО3** (функциональный)  Применять алгоритмы защиты информации используя криптографические методы, знания по работе с программами информационной безопасности | **3.1** – интепретировать алгоритмическое преобразование данных;  **3.2** – применять методы асимметричной и симметричной криптографии для защиты файла любого формата;  **3.3** – обеспечить защиту информации используя программы ЗИ. |
| **РО4** (системные): реализовать прикладные задачи защиты информации на базе языков программирования и пакетов прикладных программ криптозащиты. | **4.1** – интепретировать криптографические методы защиты информации;  **4.2**– применять современные методы криптозащиты при исследовании и проектировании защитных систем. |
| **РО5** (системный) Владеть навыками построения криптосистем и оценки их эффективности.  - навыками выбора технических средств, обеспечения их аппаратной сов-местимости и конфигурации. | **5.1** – интепретировать методы построения криптосистем и оценки их эффективности;  **5.2**– решать задачи формирования и проверки электронной цифровой подписи. |
| **Пререквизиты и постреквизиты** | **Пререквизиты:** Дискретная математика, информатика, алгебра.  **Постреквизиты:** Технические средства и методы защиты информации. | |
| **Литература и ресурсы** | **Литература**:  Основная:   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.   Дополнительная:  1. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.  2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.   1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2002. – 480 с.   **Список необходимых средств и материалов обучения:**   * Компьютер с установленным программным обеспечением; * Выход в интернет. * Ресурсы:   **- Програмнное обеспчение и Интернет- ресурсы:**  Microsoft Office Word, Visual Studio  **- базы данных, нформационно-справочные и поисковые системы:**  интернет ресурсы; основы криптографии и защиты информации.  **Онлайн достижимость:** дополнительные учебные материалы, домашние задания и проекты можно найти на своих страницах (УМКД) на сайте univer.kaznu.kz. | |

|  |  |
| --- | --- |
| **Академическая политика курса в контексте университетских морально-этических ценностей** | **Правила академического поведения:**   1. К каждому аудиторному занятию (семинарские) вы должны подготовиться заранее, согласно графику, приведенному ниже. Подготовка задания должна быть завершена до аудиторного занятия, на котором обсуждается тема. 2. **Академические ценности:** 3. Семинарские занятия, СРМ должны носить самостоятельный, творческий характер 4. Недопустимы плагиат, подлоги, использование шпаргалок, списывание на всех этапах контроля знаний   Обучающиеся с ограниченными возможностями могут получать консультационную помощь по Э- адресу: enlik\_89@mail.ru |
| **Политика оценивания и аттестации** | **Критериальное оценивание:** оценивание результатов обучения в соотнесенности с дескрипторами (проверка сформированности компетенций на рубежном контроле и экзаменах).  **Суммативное оценивание:** оценивание активности работы в аудитории; оценивание выполненного задания. |

**Календарь (график) реализации содержания учебного курса**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Неделя | Название темы | Результаты обучения (РО) | Индикаторы достижения РО | Кол-во часов | Максбалл | Форма оценки знаний | Форма проведения занятия  /платформа |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |  |
| **I** | **Модуль - 1** | | | | | |  |
| 1 | **Л1.** Цель и задачи курса. Криптография и криптоанализ: история, философия, подходы. | РО 1 | 1.1 | 1 | 1 | Презентация Беседа по материалу лекции | Видеолекция/Zoom |
| 1 | **СЗ:** Классические шифры. Математические модели открытого текста. Шифры перестановки. Шифры замены. Математическая модель шифра замены. Классификация шифров замены. Часть 1. | РО 1 | 1.1 | 1 | 2 | Презентация Беседа-опрос | Zoom |
| 1 | **ЛЗ.** Задания на криптоанализ классических шифров. Шифр столбцовой перестановки. Шифр двойной перестановки. | РО 1 | 1.1 | 2 | 10 | Презентация Беседа-опрос | Zoom |
| 1 | **СРСП 1:** Консультация. Знакомство с графиком сдачи СРСП. История криптоанализа в Казахстане. | РО1 | 1.1 | 10 | 10 | Презентация Беседа-опрос | Zoom |
| 2 | **Л2.** Обзор современных направлений в криптографии и криптоанализе. Универсальные методы криптоанализа. | РО 1 | 1.1 | 1 | 1 | Презентация Беседа по материалу лекции | Zoom |
| 2 | **СЗ:** Классические шифры. Математические модели открытого текста. Шифры перестановки. Шифры замены. Математическая модель шифра замены. Классификация шифров замены. Часть 2. | РО1 | 1.1 | 1 | 2 | Беседа-опрос | Zoom |
| 2 | **ЛЗ.** Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации. | РО 1 | 1.1  1.2 | 2 | 10 | Презентация Беседа-опрос | Zoom |
| 3 | **Л3.** Теоретические основы построения криптографических систем с секретным ключом. Принцип Керхгоффа. Типы криптографических систем. | РО 1 | 1.2  1.3 | 1 | 1 | Презентация Беседа по материалу лекции | Zoom |
| 3 | **СЗ.** Абсолютно стойкие криптографические системы. Вычислительно стойкие шифры. | РО 1 | 1.1  1.2  1.3 | 1 | 2 | Презентация Беседа-опрос | Zoom |
| 3 | **ЛЗ.** Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей. |  |  | 2 | 15 | Презентация Беседа-опрос | Zoom |
| **II** | **Модуль – II** | | | | | |  |
| 4 | **Л4.** Криптоанализ симметричных криптосистем: блочные шифры. Структура алгоритмов блочного шифрования. Определение алгоритма блочного шифрования. Схема Фейстеля. Принципы построения блочных шифров. | РО 2 | 2.1 | 1 | 1 | Презентация Беседа по материалу лекции | Zoom |
| 4 | **СЗ.** Число раундов шифрования. Требования, предъявляемые к функции преобразования F. Структура S-блоков. Алгоритм вычисления ключа. | РО 2 | 2.1 | 1 | 2 | Презентация Беседа-опрос | Zoom |
| 4 | **ЛЗ.** Сети Фейстеля. Программная реализация сети Фейстеля. | РО 2 | 2.1  2.2 | 2 | 10 | Презентация Беседа-опрос | Zoom |
| 4 | **СРСП 2:** Другие известные алгоритмы блочного шифрования. RC 5. IDEA. SAFER. Blowfish. | РО 2 | 2.1  2.2 |  | 15 | Презентация Беседа-опрос | Zoom |
| 5 | **Л5.** Стандарты блочного шифрования. Федеральный стандарт США- DES. Упрощенный DES. Вычисление ключей S-DES. | РО 2 | 2.2 | 1 | 1 | Презентация Беседа по материалу лекции | Zoom |
| 5 | **СЗ.:** Стандарт России – ГОСТ 28147-89. | РО 2 | 2.1  2.2 | 1 | 2 | Презентация Беседа-опрос | Zoom |
| 5 | **ЛЗ.** Вопросы и задания по стандартам блочного шифрования. | РО 2 | 2.1  2.2 | 2 | 15 | Презентация Беседа-опрос | Zoom |
|  | **РК 1** |  |  |  | **100** | **Контрольный опрос** |  |
| 6 | **Л6.** Алгоритм шифрованияAES. Алгоритм шифрования S\_AES. | РО 2 | 2.1  2.2 | 1 | 1 | Презентация Беседа по материалу лекции | Zoom |
| 6 | **СЗ.** Криптоанализ алгоритма AES. | РО 2 | 2.1  2.2 | 1 | 2 | Презентация Беседа-опрос | Zoom |
| 6 | **ЛЗ.** Стандарт симметричного шифрования AES. Программная реализация. | РО 2 | 2.1  2.2 | 2 | 10 | Презентация Беседа-опрос | Zoom |
| **III** | **Модуль - III** | | | | | |  |
| 7 | **Л7.** Функции генераторов псевдослучайных последовательностей в системах защиты информации. Требования к генераторам ПСП. Криптостойкость. Принципы построения генераторов ПСП | РО 3 | 3.1 | 1 | 1 | Презентация Беседа по материалу лекции | Zoom |
| 7 | **СЗ.** Классификация генераторов ПСП. Криптографические генераторы ПСП. | РО 3 | 3.1 | 1 | 2 | Презентация Беседа-опрос | Zoom |
| 7 | **ЛЗ.** Конгруэнтные генераторы ПСП. Период и потенциал линейных конгруэнтных генераторов. Примеры и задачи. | РО 3 | 3.1 | 2 | 10 | Презентация Беседа-опрос | Zoom |
| 8 | **Л8.** Генераторы ПСП на регистрах сдвига с линейными обратными связами. | РО 3 | 3.1  3.2  3.3 | 1 | 1 | Презентация Беседа по материалу лекции | Zoom |
| 8 | **СЗ.** Комбинирующие генераторы РСЛОС. Генератор Геффе. | РО 3 | 3.1  3.2 | 1 | 2 | Презентация Беседа-опрос | Zoom |
| 8 | **ЛЗ.** Регистры сдвига с линейной обратной свзяью как генераторы псевдослучайных чисел. | РО 3 | 3.1  3.2  3.3 | 2 | 10 | Презентация Беседа-опрос | Zoom |
| 8 | **СРСП3.** Потоковые шифры на основе РСЛОС | РО 3 | 3.1  3.2  3.3 |  | 15 | Фронтальный и индивидуальный опрос | Zoom |
| **IV** | **Модуль - IV** | | | | | |  |
| 9 | **Л9.** Методика оценки качества генераторов ПСП. Графические тесты. Гистограмма распределения элементов. Распределение на плоскости. Проверка серий. | РО 3 | 3.1  3.2 | 1 | 1 | Презентация Беседа по материалу лекции | Zoom |
| 9 | **СЗ.** Проверка на монотонность | РО 3 | 3.1  3.2 | 1 | 2 | Презентация Беседа-опрос | Zoom |
| 9 | **ЛЗ.** Автокорреляционная функция. | РО 3 | 3.1  3.2 | 2 | 10 | Презентация Беседа-опрос | Zoom |
| 9 | **СРСП 4:** Программные реализации тестов. | РО 3 | 3.1  3.2 |  | 20 | Презентация Беседа-опрос | Zoom |
| 10 | **Л10.**  **Оценочные тесты.** Сведения из теории вероятностей и математической статистики. | РО 3 | 3.1  3.2 | 1 | 1 | Презентация Беседа по материалу лекции | Zoom |
| 10 | **СЗ.** Подборка тестов Д. Кнута. Проверка несцепленных серий. Проверка интервалов. | РО 3 | 3.1  3.2 | 1 | 2 | Презентация Беседа-опрос | Zoom |
| 10 | **ЛЗ.** Система оценки статистических свойств «DIEHARD». | РО 3 | 3.1  3.2 | 2 | 10 | Фронтальный и индивидуальный опрос | Zoom |
|  | **Midterm** |  |  |  | **100** | **Фронтальный и индивидуальный опрос** | Zoom |
| 11 | **Л11.** Руководство НИСТ. Общие положения. Частотный тест. Частотный тест в подпследовательностях. | РО 3 | 3.1  3.2 | 1 | 1 | Презентация Беседа по материалу лекции | Zoom |
| 11 | **СЗ.** Тест «дырок». Тест «блоков» в подпоследовательностях. | РО 3 | 3.1  3.2 | 1 | 2 | Презентация Беседа-опрос | Zoom |
| 11 | **ЛЗ.** Посимвольная проверка. Проверка частот. Оценка результатов тестирование. |  |  | 2 | 10 | Презентация Беседа-опрос | Zoom |
| **V** | **Модуль V** | | | | | |  |
| 12 | **Л12.** Линейный криптоанализ блочных алгоритмов шифрования. Общие сведения о линейном криптоанализе. | РО 4 | 4.1 | 1 | 1 | Презентация Беседа по материалу лекции | Zoom |
| 12 | **СЗ.** Применение линейного криптоанализа к алгоритмам шифрования. | РО 4 | 4.1 | 1 | 2 | Презентация Беседа-опрос | Zoom |
| 12 | **ЛЗ.** Вопросы по линейному криптоанализу к алгоритмам шифрования. | РО 4 | 4.1 | 2 | 10 | Презентация Беседа-опрос | Zoom |
| 12 | **СРМП 5.** Дифференциальный криптоанализ алгоритма шифрования RC 5. | РО 4 | 4.1 | 1 | 35 | Фронтальный и индивидуальный опрос | Zoom |
| 13 | **Л13** Дифференциальный криптоанализ блочных алгоритмов шифрования. Общие сведения о дифференциальном криптоанализе. | РО 4 | 4.1  4.2 | 1 | 1 | Презентация Беседа по материалу лекции | Zoom |
| 13 | **СЗ.** Применение дифференциального криптоанализа к алгоритмам шифрования. | РО 4 | 4.1  4.2 | 1 | 2 | Презентация Беседа-опрос | Zoom |
| 13 | **ЛЗ.** Вопросы по дифференциальному криптоанализу к алгоритмам шифрования. |  |  | 2 | 10 | Презентация Беседа-опрос | Zoom |
| **VI** | **Модуль - VI** | | | | | |  |
| 14 | **Л14.** Алгебраический криптоанализ. Основная идея. Метод алгебраического криптоанализа. | РО 5 | 5.1 | 1 | 1 | Презентация Беседа по материалу лекции | Zoom |
| 14 | **СЗ.** Криптоанализ поточного шифра. Рассмотрение примеров. | РО 5 | 5.1 | 1 | 2 | Презентация Беседа-опрос | Zoom |
| 14 | **ЛЗ.** Вопросы по алгебраическому криптоанализ. | РО 5 | 5.1 | 2 | 10 | Презентация Беседа-опрос | Zoom |
| 15 | **Л15.** Слайдовый криптоанализ. Основная идея. Методы. | РО 5 | 5.1  5.2 | 1 | 1 | Презентация Беседа по материалу лекции | Zoom |
| 15 | **СЗ.** Алгоритм слайдового криптоанализа. | РО 5 | 5.1  5.2 | 1 | 2 | Презентация Беседа-опрос | Zoom |
| 15 | **ЛЗ.** Криптоанализ шифра KeeLog | РО 5 | 5.1  5.2 | 2 | 10 | Презентация Беседа-опрос | Zoom |
| 15 | **СРСП.** Прием СРС | РО 5 | 5.1  5.2 | 1 |  | Фронтальный и индивидуальный опрос | Zoom |
|  | **РК 3** |  |  |  | **100** | **Контрольный опрос** | **Zoom** |
|  | **Экзамен** |  |  |  | 100 | Контрольный опрос |  |

Декан ф-та, к.ф.м.н., доцент  Урмашев Б. А.

Председатель метод бюро Байшоланова К. С.

Заведующий кафедрой Мусиралиева Ш.Ж.

Лектор Бегимбаева Е.Е.