Силлабус
Весенний семестр 2020-2021 у.г.
По образовательной программе «5В100200 – Системы информационной безопасности»

Код дисциплины	Название дисциплины	СРМ	Кол-во часов			Кол-во кредитов	СРМП
			Лекц.	Практ.	Лабор.		
	Кибербезопасность	85	15		30	5	5

Академическая информация о курсе

Вид обучения	Тип/характер курса	Тип лекции	Типы практических занятий	Кол-во СРМ	Тип итогового контроля
Онлайн / объединенная	теоретический	Аналитическая	Лабораторные работы	три	Тест
Лектор	**PhD. Рахимова Диана Рамазановна**			**Оф./с.**	По расписанию
e-mail	E-mail: diana.rakhimova@kaznu.kz				
Телефон	Телефон: 8777-2420775				

Академическая презентация курса

Цель дисциплины	Ожидаемые результаты обучения (РО)	Индикаторы достижения РО (на каждый РО не менее 2-х индикаторов)
Помощь в овладении теоретическими знаниями и формировании практических умений и навыков в области обеспечения надежности и безопасности программного обеспечения (ПО) современных технических систем, и прежде всего в освоении комплекса мер, методов и способов защиты ПО от непреднамеренных и преднамеренных программных воздействий.	**РО** 1 (когнитивный) Знать основы деятельности государства в условиях информационного противоборства; основные положения теории надежности и безопасности ИС; нормативные правовые документы в области функциональной надежности, функциональной и информационной безопасности; математические модели надежности и безопасности ПО; модели и методы защиты операционных систем; основные проектные решения, средства и методы защиты ПО от непреднамеренных дефектов и вредоносных программ	**1.1** - осуществлять критический анализ проблемных ситуаций на основе системного подхода **1.2** - вырабатывать программу действий для проблемных ситуаций на основе системного подхода **1.3** - управлять проектом защиты ПО на всех этапах его жизненного цикла
	РО 2 (функциональный) Применять существующие методы защиты информации от несанкционированного доступа без снижения их стойкости вследствие принятия неправильных эксплуатационных решений	**2.1** –решать типовые задачи с помощью методов надежности технических систем и защиты информации от несанкционированного доступа; **2.2** –прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты
	РО 3 (функциональный) Применять современные методы и методики защиты ПО от непреднамеренных дефектов и вредоносных программ, от несанкционированного исследования, копирования, распространения и использования	**3.1** –проводить обоснование состава, характеристик и функциональных возможностей систем, средств и технологий обеспечения информационной безопасности объектов защиты на основе казахстанских и международных стандартов; **3.2** –разрабатывать и проводить испытания систем, средств и технологий обеспечения информационной безопасности с применением соответствующих физических и математических методов, технических и программных средств; **3.3** –организовать работу по созданию, модернизации и вводу в эксплуатацию систем, средств и технологий

		обеспечения информационн ой безопасности в соответствии с правовыми нормативными актами и нормативными методическим и документами КНБ и Правительства Республики Казахстан
	РО 4 (системный) Владеть методами разработки и использования защищенных программных средств	**4.1** – проводить анализ процесса функционирования объекта защиты совместно с применяемыми информационными технологиями и техническими средствами с целью определения возможных источников информационных угроз, их вероятных целей и тактики воздействия на объект защиты; **4.2** – формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта и его информационных составляющих, с целью повышения их устойчивости к деструктивным воздействиям.
	РО 5 (системный) Владеть навыками эксплуатации защищенных программных средств, получивших широкое применение в современных автоматизированных системах.	**5.1** – разработать комплекс организационных и технических мер по обеспечению информационной безопасности объекта информатизации **5.2** – провести выбор необходимых технологий и технических средств по обеспечению информационной Безопасности объекта информатизации, организовать их внедрение и последующее сопровождение **5.3** – организовать и сопровождать аттестацию объектов информатизации в соответствии с нормативными документами.
Пререквизиты и постреквизиты	**Пререквизиты:** нет **Постреквизиты:** все профилирующие дисциплины 7 семестра и практики семестров	
Литература и ресурсы	**Литература**: **Основная:** 1. Адаменко М.В., Основы классической криптологии: секреты шифров и кодов / Адаменко М.В. - М. : ДМК Пресс, 2012. - 256 с. - ISBN 978-5-94074-456-6 2. Blake Barry J. Secret Language: Codes, Tricks, Spies, Thieves, and Symbols - Oxford University Press, 2011. - 288 p. - ISBN-13: 978-0199691623 3. Chatterjee S., Sarkar P. Identity-Based Encryption. - Springer, 2011. - 193 p. - ISBN:1441993827 4. Голиков А.М. Математические основы криптологии. Учебное пособие / А.М.Голиков. - Томск: Томск, гос. ун-т систем упр. и радиоэлектроники, 2016. - 428 с **Дополнительная:** указана в методических указаниях по выполнению СРМ **Список необходимых средств и материалов обучения:** • Текстовые и графические редакторы (различных масштабов и тематики) • Компьютерные программы тестирования ПО **Ресурсы:** - **Програмнное обеспчение и Интернет- ресурсы:** Microsoft Office, Power Point, Adobe Reader, Paint. - **базы данных, нформационно-справочные и поисковые системы:** специализированные веб-сайты и базы данных в интернет указаны в методических	

	указаниях по выполнению СРМ **Онлайн достижимость:** дополнительные учебные материалы, задания для СРМ и лабораторных работ 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 (лекции, лабораторной работе) вы должны подготовиться заранее, согласно графику, приведенному ниже. Подготовка задания должна быть завершена до аудиторного занятия, на котором обсуждается тема. **2. Академические ценности:** 1. Лабораторные занятия, СРМ должны носить самостоятельный, творческий характер 2. Недопустимы плагиат, подлоги, использование шпаргалок, списывание на всех этапах контроля знаний Обучающиеся с ограниченными возможностями могут получать консультационную помощь по Э- адресу diana.rakhimova@kaznu.kz
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	Макс балл	Форма оценки знаний
1	2	3	4	5	6	7
I	**Модуль - Основы кибербезопасности.**					
1	**Лекция (**аналитическая**):** Введение. Примеры шифров.	РО 1	1.1	1	2	
1	**Лабораторное занятие:** Классические шифры 1 **Тип задания:** Составление отчета	РО 1	1.1	2	10	Отчет
1	**СРМ- 1.** Основы криптоанализа Задание 1. Введение. Примеры шифров. **Тип задания:** Составление отчета	РО 1	1.1; 1.2; 1.3	6	8	Отчет
2	**Лекция (**аналитическая**):** Стойкость шифров	РО 1	1.1	1	2	Беседа-опрос
2	**Лабораторное занятие:** Классические шифры 2 **Тип задания:** Составление отчета	РО 1	1.1	2	10	Отчет
2	**СРМ- 1.** Основы криптоанализа Задание 2. Стойкость шифров. **Тип задания:** Составление отчета	РО 1	1.1; 1.2; 1.3	6	8	Отчет
3	**Лекция** (аналитическая) Метод полного перебора	РО 1	1.2; 1.3	1	2	Беседа-опрос
3	**Лабораторное занятие:** Классические шифры 3 **Тип задания:** Составление отчета	РО 1	1.2; 1.3	4	10	Отчет
3	**СРМ- 1.** Основы криптоанализа Задание 3. Метод полного перебора. **Тип задания:** Составление отчета	РО 1	1.1; 1.2; 1.3	6	8	Отчет
4	**Лекция** (аналитическая) Аналитический метод	РО 1	1.2; 1.3	1	2	Беседа-опрос
4	**Лабораторное занятие:** Шифр столбцовой перестановки 1 **Тип задания:** Составление отчета	РО 1	1.2; 1.3	2	10	Отчет
4	**СРМП 1** - Проведение взаимного обсуждения и консультации по **СРМ 1**	РО 1	1.1; 1.2; 1.3	1	0	Беседа
4	**СРМ- 1.** Основы криптоанализа Задание 4. Аналитический метод **Тип задания:** Составление отчета	РО 1	1.1; 1.2; 1.3	5	8	Отчет

5	**Лекция** (аналитическая) Метод «встреча по середине»	РО 1	1.2; 1.3	1	2	Беседа-опрос
5	**Лабораторное занятие:** Шифр столбцовой перестановки 2	РО 1; РО 2	1.3; 2.1; 2.2	2	10	Отчет
	Тип задания: Составление отчета					
5	**СРМ- 1.** Основы криптоанализа Задание 5. Метод «встреча по середине» **Тип задания:** Составление отчета	РО 1	1.1; 1.2; 1.3	5	8	Отчет
5	**СРМП 2 -** Прием и оценка задания по **СРМ 1**	РО 1; РО 2	1.2; 1.3; 2.1; 2.2	1	0	Собеседование и защита
5	**РК 1 накопительный**				100	
II	**Модуль – Универсальные методы защиты**					
6	**Лекция** (аналитическая) Метод «разделяй и побеждай»	РО 2	2.1	1	2	Беседа-опрос
6	**Лабораторное занятие:** Шифр двойной перестановки 1 **Тип задания:** Составление отчета	РО 2	2.1	2	10	Отчет
6	**СРМ- 2.** Универсальные методы криптоанализа Задание 1. Метод «разделяй и побеждай». **Тип задания:** Составление отчета	РО 2; РО 4	2.1; 2.2; 4.1	6	8	Отчет
7	**Лекция (**аналитическая**)** Методы криптоанализа при неравновероятностной гамме. Расстояние единственности	РО 2	2.2	1	2	Беседа-опрос
7	**Лабораторное занятие:** Шифр двойной перестановки 2 **Тип задания:** Составление отчета	РО 2; РО 3; РО 4	2.2; 3.1; 4.1	2	10	Отчет
7	**СРМ- 2.** Универсальные методы криптоанализа Задание 2. Методы криптоанализа при неравновероятностной гамме. Расстояние единственности. **Тип задания:** Составление отчета	РО 2; РО 4	2.1; 2.2; 4.1	6	8	Отчет
8	**Лекция** (аналитическая) Перекрытия гаммы	РО 3	3.1; 3.2; 3.3	1	2	Беседа-опрос
8	**Лабораторное занятие:** Шифр простой замены 1 **Тип задания:** Составление отчета	РО 3	3.1; 3.2; 3.3	2	10	Отчет
8	**СРМ- 2.** Универсальные методы криптоанализа Задание 3. Перекрытия гаммы. **Тип задания:** Составление отчета	РО 2; РО 4	2.1; 2.2; 4.1	5	8	Отчет
8	**СРМП 3** Проведение взаимного обсуждения и консультации по **СРМ 2**	РО 2; РО 4	2.1; 2.2; 4.1	1	0	Беседа
9	**Лекция (**аналитическая**)** Корреляционные атаки на поточные шифры	РО 3	3.1: 3.2: 3.3	1	2	Беседа-опрос
9	**Лабораторное занятие:** Шифр простой замены 2 **Тип задания:** Составление отчета	РО 3; РО 4; РО 5	3.2; 4.1; 4.2; 5.1	2	10	Отчет
9	**СРМ- 2.** Универсальные методы криптоанализа Задание 4. Корреляционные атаки на поточные шифры. **Тип задания:** Составление отчета	РО 2; РО 4	2.1; 2.2; 4.1	6	8	Отчет
10	**Лекция** (аналитическая) Статистические модели	РО 3	3.1; 3.3	1	2	Беседа-опрос
10	**Лабораторное занятие:** Шифр простой замены 3 **Тип задания:** Составление отчета	РО 3; РО 4	3.1; 3.3; 4.2	2	10	Отчет
10	**СРМ- 2.** Универсальные методы криптоанализа Задание 5. Статистические модели. **Тип задания:** Составление отчета	РО 2; РО 4	2.1; 2.2; 4.1	6	8	Отчет
10	**Midterm накопительный**				100	

III	Модуль - Линейный криптоанализ.					
11	**Лекция** (аналитическая): Линейный криптоанализ блочных шифров	РО 4	4.1; 4.2	1	2	Беседа-опрос
11	**Лабораторное занятие:** Теория криптоанализа шифра Виженера 1 **Тип задания:** Составление отчета	РО 4	4.1; 4.2	2	10	Отчет
11	**СРМ- 3.** Линейный криптоанализ Задание 1. Линейный криптоанализ блочных шифров. **Тип задания:** Составление отчета	РО 2; РО 4	2.1; 2.2; 4.1	5	8	Отчет
11	**СРМП 4** – Проведение взаимного обсуждения и консультации по **СРМ 3**	РО 3; РО 4	3.1; 3.2; 3.3; 4.1; 4.2	1	0	Беседа
12	**Лекция** (аналитическая): Дифференциальный криптоанализ	РО 4	4.1; 4.2	1	2	Беседа-опрос
12	**Лабораторное занятие:** Теория криптоанализа шифра Виженера 2 **Тип задания:** Составление отчета	РО 4; РО 5	4.1; 4.2; 5.1; 5.2	2	10	Отчет
12	**СРМ- 3.** Линейный криптоанализ Задание 2. Дифференциальный криптоанализ. **Тип задания:** Составление отчета	РО 2; РО 4	2.1; 2.2; 4.1	6	8	Отчет
13	**Лекция** (аналитическая): Метод коллизий для хэш-функций	РО 5	5.1; 5.2	1	2	Беседа-опрос
13	**Лабораторное занятие:** Теория криптоанализа шифра Виженера 3 **Тип задания:** Составление отчета	РО 5	5.1; 5.2	2	10	Отчет
13	**СРМ- 3.** Линейный криптоанализ Задание 3. Метод коллизий для хэш-функций. **Тип задания:** Составление отчета	РО 2; РО 4	2.1; 2.2; 4.1	5	8	Отчет
13	**СРМП 5** - Проведение взаимного обсуждения и консультации по **СРМ 3**	РО 3; РО 4	3.1; 3.2; 3.3; 4.1; 4.2	1	0	Беседа
14	**Лекция** (аналитическая): Анализ схем шифрования, использующих многократно один блочный шифр	РО 5	5.1; 5.2; 5.3	1	2	Беседа-опрос
14	**Лабораторное занятие:** Криптоанализ английского текста 1 **Тип задания:** Составление отчета	РО 5	5.1; 5.2; 5.3	2	10	Отчет
14	**СРМ- 3.** Линейный криптоанализ Задание 4. Анализ схем шифрования, использующих многократно один блочный шифр. **Тип задания:** Составление отчета	РО 2; РО 4	2.1; 2.2; 4.1	5	8	Отчет
15	**Лекция** (аналитическая): Атака на тройной DES с помощью линейного криптоанализа.	РО 5	5.1; 5.2; 5.3	1	2	Беседа-опрос
15	**Лабораторное занятие:** Криптоанализ английского текста 2 **Тип задания:** Составление отчета	РО 5	5.1; 5.2; 5.3	2	10	Отчет
15	**СРМ- 3.** Линейный криптоанализ Задание 5. Атака на тройной DES с помощью линейного криптоанализа. **Тип задания:** Составление отчета	РО 2; РО 4	2.1; 2.2; 4.1	6	8	Отчет
15	**РК 2 накопительный**				100	

Декан ф-та, профессор Б.А. Урмашев
Председатель методбюро Ф.Р. Гусманова
Заведующий кафедрой Ш.Ж. Мусиралиева
Лектор Д.Р. Рахимова