

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ
ОШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ, ФИЗИКИ, ТЕХНИКИ И ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ
КАФЕДРА АВТОМАТИЗИРОВАННЫХ СИСТЕМ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

СОГЛАСОВАНО
Председатель УМС института доцент
Э.А. Мамазияева

Протокол №1, 26.08.2024

УТВЕРЖДЕНО
Заведующий кафедры,
доцент А.Ж. Кудуев

Протокол №1, 26.08.2024

ПРОГРАММА ОБУЧЕНИЯ
(Syllabus)

Специальность (направление)	Математическое обеспечение и администрирование информационных систем	Код курса	510700
Язык обучения	Русский, кыргызский	дисциплина	Безопасность жизнедеятельности
Акад. год	2024-2025-г.	Количество кредитов	4
преподаватель	Дарбанов Э.О.	семестр	VII
e-mail	edarbanov@oshsu.kg	Расписание по ссылке https://myedu.oshsu.kg/	
Консультации (время/ауд)	Среда, 318 Кабинет, время: 16:40 - 18:10	Место (здание/ауд.)	ОшГУ глав. Корпус, кабинет №318
Форма обучения (дневная/заочная/вечерняя/дистанционная)	дневная	Тип курса: (обязательный/ элективный)	обязательный

Ош, 2024

ДАННЫЕ О ПРЕПОДАВАТЕЛЕ

Дарбанов Эльстан Ооматбекович – преподаватель кафедры АСЦТ, институт МФТИТ в ОшГУ. Стаж работы – 8. Образование высшее, окончил 2024 г. факультет физики – математики и информационных технологий ОшГУ.

Место работы: 723500. Главный корпус ОшГУ, улица Ленина 331, каб. 216.

Мобильный телефон: (0771) 30-24-14

E-mail: edarbanov@oshsu.kg



Характеристика курса:

Курс направлен на формирование у студентов целостного понимания обеспечения безопасности в ИТ-сфере и подготовку их к работе в условиях повышенных требований к защите информации.

Цель курса:

Курс "Безопасность жизнедеятельности" направлен на развитие умений и навыков обеспечения безопасности в профессиональной деятельности. Основное внимание уделяется защите от угроз и рисков в сфере информационных технологий и управлению этими рисками в современном ИТ-контексте.

Пререквизиты	Основы информатики: Знание базовых концепций и принципов работы с информационными системами. Компьютерные сети: Понимание основ работы компьютерных сетей и протоколов связи. Операционные системы: Знание принципов работы операционных систем и их внутреннего устройства.	
Со-реквизиты	Информационные системы и технологии: Знание и понимание использования информационных систем и технологий для решения задач. Базы данных: Основы проектирования и работы с базами данных.	
Постреквизиты	Информационная безопасность: Глубокие знания и навыки в области защиты информации и управления безопасностью. Анализ и проектирование информационных систем: Навыки анализа требований и проектирования систем с учетом аспектов безопасности.	
Результаты обучения дисциплины		
К концу курса студент:		
РО (результат обучения) ООп	РО дисциплины	Компетенции
Результаты обучения 6. Владеет навыками администрирования информационных систем, включая настройку ОС, веб-серверов, обслуживание ПО и защиту данных.	иметь представление: <ul style="list-style-type: none">о подходах к решению сложных задач с использованием средств вычислительной техники;о фундаментальных свойствах алгоритмов;о развитии программирования как деятельности;об эволюции языков программирования;о развитии технологий программирования. уметь:	ИК-3. Владеет основными методами, способами и средствами получения, хранения и переработки информации, навыками работы с компьютерами как средством управления информацией, в том числе в глобальных компьютерных сетях и корпоративных информационных системах.

	пользоваться современными аппаратными средствами; согласованно решать задачи разработки эффективных моделей, данных и алгоритмов их обработки при создании прикладного программного обеспечения, а также получать программные реализации на языках высокого уровня.	• ПК-20. Владеет навыками использования основных моделей информационных технологий и способов их применения для решения задач в предметных областях
--	--	---

Календарно-тематический план лабораторных занятий						
№	Название темы	Количество часов/баллы				Литература
		Лекц. (20ч)	ТКсп (86)	Лаб. (28ч)	СРСР (126)	
Модуль 1: Основы безопасности и охрана труда						
1	Лекция 1: Введение в дисциплину "Безопасность жизнедеятельности" и основные понятия безопасности	2	5/5	2		ЭР [1,2], ЭУ [1:23-46 стр.]
	Практическое занятие №1 "Введение в дисциплину 'Безопасность жизнедеятельности' и основные понятия безопасности"			2		
2	Лекция 2: Факторы производственной среды и их влияние на человека	2	5/5	2		ЭР [3,4], ЭУ [2:47-68 стр.]
	Практическое занятие №2 "Факторы производственной среды и их влияние на человека"			2		
3	Лекция 3: Охрана труда и производственная безопасность в сфере ИТ	2	5/5	2		ЭР [5,6], ЭУ [3:69-90 стр.]
	Практическое занятие №3 по теме: Охрана труда и производственная			2		

	безопасность в сфере ИТ с использованием метода квеста					
4	Лекция 4: Эргономика и организация рабочего места ИТ-специалиста	2	5/5	2		ЭР [7,8], ЭУ [4:91-112 стр.]
	Практическое занятие №4 по теме: Эргономика и организация рабочего места ИТ-специалиста			2		
ТК1 Средние накопленные баллы		5/5				
Итого за ТК1		10				
5	Лекция 5: Пожарная безопасность в ИТ-организациях	2	5/5	2		ЭР [9,10], ЭУ [5:113-134 стр.]
	Практическое занятие №5 по теме: Пожарная безопасность в ИТ-организациях			2	2	
ТК2 Средние накопленные баллы		5/5				
Итого за ТК2		10				
Модуль 2: Информационная безопасность и управление рисками						
6	Лекция 6: Чрезвычайные ситуации и методы защиты от них	2		2		ЭР [11,12], ЭУ [6:135-156 стр.]
	Практическое занятие №6 Чрезвычайные ситуации и методы защиты от них			2		
7	Лекция 7: Информационная безопасность: основные угрозы и защита	2		2		ЭР [13,14], ЭУ [7:157-178 стр.]
	Практическое занятие №7			2		

	Информационная безопасность: основные угрозы и защита					
8	Лекция 8: Программные и аппаратные методы защиты информации	2		2		ЭР [15,16], ЭУ [8:179-200 стр.]
	Практическое занятие №8 Программные и аппаратные методы защиты информации			2	2	
ТК3 Средние накопленные баллы		5/5				
Итого за ТК3		10				
9	Лекция 9: Организация безопасного программирования	2		2		ЭР [17,18], ЭУ [9:201-220 стр.]
	Практическое занятие №9 Организация безопасного программирования			2	2	
10	Лекция 10: Оценка и управление рисками в сфере ИТ	2		2	2	ЭР [19,20], ЭУ [10:221-240 стр.]
	Практическое занятие №10 Оценка и управление рисками в сфере ИТ			2	2	
	Практическое занятие №11, №12: Квест по оценке и управлению рисками в сфере ИТ			4	2	
	Практическое занятие №11 и №12: Кейс по оценке и управлению рисками по безопасности работников в сфере ИТ			4		
ТК4 Средние накопленные баллы		5/5				
Итого за ТК4		10				
Итого	20	28				

Критерии оценивания лабораторных работ

Критерий	Максимальный балл	Описание
Полнота выполнения задания	4 балла	Соответствие требованиям, выполнение всех пунктов задания
Глубина анализа	2 балла	Обоснованные выводы, проработанный анализ и логика
Качество оформления	2 балла	Грамотность, структурированность, логичное изложение
Креативность и оригинальность	2 балла	Использование нестандартных решений, применение реальных кейсов

Итоговая оценка

- 9-10 баллов (отлично)** – Работа полностью соответствует требованиям, глубокий анализ, грамотное оформление.
 - 7-8 баллов (хорошо)** – В основном все выполнено правильно, но есть небольшие недочеты.
 - 5-6 баллов (удовлетворительно)** – Частично выполненное задание, есть пробелы в анализе или оформлении.
- 0-4 балла (неудовлетворительно)** – Работа не соответствует требованиям, допущены серьезные ошибки.

План организации СРСП (12 часов)							
№	Тема	Задание для СРСП	Часы	Оценочные средства	Балл Лек./Лаб.	Литер., сайт, ссылка	Срок сдачи
1	Изучение теоретических основ ИБ и рисков	Самостоятельное изучение материалов по ISO 27001, GDPR и основам управления рисками	2	Устный опрос, тест	1/0	ЭР [1], ЭУ [1]	05.04
2	Анализ кейсов по информационно й безопасности	Работа с кейсами, выявление рисков, разработка решений	2	Заполненный шаблон, анализ	0/1	ЭР [2], шаблоны кейсов	06.04
3	Индивидуальный мини-проект	Разработка политик и планов управления рисками	2	Проект, оценка преподавателем	0/1	ЭР [3], шаблоны планов	07.04
4	Рефлексия и анализ проделанной работы	Свободное обсуждение, самоанализ, обсуждение с преподавателем	2	Участие в обсуждении, выводы	1/0	—	08.04

5	Практика: кейсовый анализ	Идентификация рисков, план реагирования	2	Проверка кейса, краткий отчёт	0/1	ЭР [4], матрицы рисков	09.04
6	Подготовка презентации и отчёта	Подготовка финального отчета и слайдов	2	Защита, отчёт	1/1	ЭР [5], PowerPoint шаблоны	1

План организации СРС (60 часов)							
№	Тема	Задание для СРС	Часы	Оценочные средства	Балл Лек./Лаб.	Литер., сайт, ссылка	Срок сдачи
1	Теоретические основы информационной безопасности	Конспект, онлайн-тест	10	Тестирование, устный опрос	1/1	ЭР [1], ЭУ [1]	10.03–15.03
2	Анализ угроз и рисков: кейсы и сценарии	Анализ кейсов, мини-эссе	10	Проверочная работа, обсуждение	0/1	ЭР [2], ЭУ [1]	17.03–22.03
3	Разработка политики безопасности	Проект, оформление документа	15	Мини-проект, защита	0/1	ЭР [3], ЭУ [2]	24.03–30.03
4	Реализация мер защиты (аутентификация, шифрование и др.)	Демонстрация, скринкаст	10	Практическая работа, отчёт	1/1	ЭР [4], сайт OWASP	01.04–06.04
5	Тестирование и оценка эффективности защиты	Протокол, журнал уязвимостей	10	Проверка, отчёт	1/1	ЭР [5], NIST SP 800-30	08.04–13.04
6	Итоговая презентация проекта	Презентация + письменный отчёт	5	Защита, презентация	1/1	ЭР [6], шаблоны	15.04–20.04

Ресурсы:

- Учебники и учебные материалы по безопасности данных и управлению рисками.
- Стандарты и нормативные документы.
- Примеры кейсов и шаблоны для анализа и разработки.
- Инструменты для защиты данных, тестирования и разработки.
- Средства для создания и проведения презентаций (PowerPoint, Google Slides и др.).

Ожидаемые результаты:

- Глубокое понимание теоретических и практических аспектов безопасности данных.
- Навыки разработки и внедрения планов управления рисками и политик безопасности.
- Практический опыт реализации решений и оценки их эффективности.
- Способность подготовить и представить результаты своей работы.

Политика курса

Основные требования к компонентам курса и его изучению:

- студент должен посещать занятия, принимать активное участие в работе группы при выполнении СРСП и СРС и на лабораторных занятиях;
- на лекционных занятиях делать записи содержания лекций, внимательно слушать, не нарушая дисциплину;
- на практическом занятии важно не только выступать, но и внимательно слушать своих сокурсников, оценивать их ответы, вести запись новой информации;

Система оценки

Декларация об академической честности: Студенты, проходящие этот курс, должны подать декларацию, требующую от них соблюдать политику университета в отношении академической честности. Положение «Организация образовательного процесса в ОшГУ» А-2024-0001, 2024.01.03.2024

Баллы за курс состоят из (100 баллов):

Название контроля	Баллы
ТК ₁	10
ТК ₂	10
СРСП ₁ +СРС ₁	10
РК ₁	20
1 модуль (М1)	50
ТК ₃	10
ТК ₄	10
СРСП ₂ +СРС ₂	10
РК ₂	20
1 модуль (М2)	50
Экзамен (100б)	100
$ИЭ=(М1+М2+Э)/2$	

Карта накопления баллов по дисциплине

Модуль 1 (30 б.)										
	ТК-1(30 б.)				ТК-2(30 б.)				РК1	М1
	лек	лаб	срс		лек	лаб	срс			
темы	30 б.	30 б.	30 б.	темы	30 б.	30 б.	30 б.	темы		
Т-1	1	1	1	Т-1	1	1	1	Т-1	30 б.	30 б.
...		
Т-N	N	N	N	Т-N	N	N	N	Т-N		
Всего	$TK1 = \frac{Лек + Лаб + CPC}{3}$			Всего	$TK2 = \frac{Лек + Лаб + CPC}{3}$			Всего	$PK1 = \frac{Лек + Лаб + CPC}{3}$	$M1 = \frac{TK1 + TK2 + TK3 + PK1}{4}$

Модуль 1 (30 б.)										
	ТК-3(30 б.)				ТК-4(30 б.)				РК2	М2
	лек	лаб	срс		лек	лаб	срс			
темы	30 б.	30 б.	30 б.	темы	30 б.	30 б.	30 б.	темы		
Т-1	1	1	1	Т-1	1	1	1	Т-1	30 б.	30 б.
...		
Т-N	N	N	N	Т-N	N	N	N	Т-N		
Всего	$TK1 = \frac{Лек + Лаб + CPC}{3}$			Всего	$TK2 = \frac{Лек + Лаб + CPC}{3}$			Всего	$PK1 = \frac{Лек + Лаб + CPC}{3}$	$M1 = \frac{TK1 + TK2 + TK3 + PK1}{4}$

Экзамен (100 б.)				
М1 (30 б.)	М2 (30б.)	ИК (30 б.)	ПБ (10 б.)	Экзамен(100б.)
30 б.	30 б.	$ИК = \frac{Лек + Лаб + СРС}{3}$	1...10	$Экз = \frac{М1 + М2 + ИК + ПБ}{3}$

Образовательные ресурсы

Электронные ресурсы (ЭР)		
№	Название	Ссылка
1	Операционная система Linux	Linux
2	Официальная документация по TCP/IP	RFC 791 TCP/IP
3	Основы безопасности жизнедеятельности	Основы безопасности
4	Учебники по безопасности на производстве	Учебники по безопасности
5	Введение в охрану труда и технику безопасности	Введение в охрану труда
6	Стандарты безопасности и охраны труда	ISO 45001
7	Управление рисками и безопасность в ИТ-организациях	Управление рисками
8	Современные системы охраны труда и безопасности	Современные системы безопасности
9	Введение в информационную безопасность в организации	Введение в ИТ безопасность
10	Основы гражданской обороны и защиты от чрезвычайных ситуаций	Гражданская оборона

Электронными учебниками (ЭУ)		
№	Название	Ссылка
1	Таненбаум Э. "Компьютерные сети"	Таненбаум - Компьютерные сети
2	Паттерсон Д., Хеннеси Дж. "Архитектура компьютера: организация и проектирование"	Архитектура компьютера
3	Виноградов И. "Память и её архитектура"	Память и её архитектура
4	Лампорт Л. "Протоколы передачи данных"	Протоколы передачи данных
5	Уильям Столлинс "Основы телекоммуникаций"	Основы телекоммуникаций
6	Розенберг А., Лавендер Д. "Облачные вычисления: технологии и модели"	Облачные вычисления