МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский технологический университет «МИСиС»

Рабочая программа дисциплины (модуля)

Системы обеспечения информационной безопасности и блокчейн

Закреплена за подразделением — Кафедра инженерной кибернетики

Направление подготовки — 01.03.04 ПРИКЛАДНАЯ МАТЕМАТИКА

Профиль — Алгоритмы и методы наукоемкого программного обеспечения

Квалификация **Бакалавр**
Форма обучения **очная**
Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 60
самостоятельная работа 48
часов на контроль 36

Формы контроля в семестрах:
экзамен 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	12			
Вид занятий	УП	РП	УП	РП
Лекции	12	12	12	12
Лабораторные	24	24	24	24
Практические	24	24	24	24
Итого ауд.	60	60	60	60
Контактная работа	60	60	60	60
Сам. работа	48	48	48	48
Часы на контроль	36	36	36	36
Итого	144	144	144	144

Программу составил(и):
Куренков Владимир Вячеславович

Рабочая программа
Системы обеспечения информационной безопасности и блокчейн

Разработана в соответствии с ОС ВО:

Самостоятельно устанавливаемый образовательный стандарт высшего образования - бакалавриат Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский технологический университет «МИСиС» по направлению подготовки 01.03.04 ПРИКЛАДНАЯ МАТЕМАТИКА (приказ от 02.04.2021 г. № 119 о.в.)

Составлена на основании учебного плана:

01.03.04 ПРИКЛАДНАЯ МАТЕМАТИКА, 01.03.04-БПМ-22.plx Алгоритмы и методы наукоемкого программного обеспечения, утвержденного Ученым советом ФГАОУ ВО НИТУ "МИСиС" в составе соответствующей ОПОП ВО 22.09.2022, протокол № 8-22

Утверждена в составе ОПОП ВО:

01.03.04 ПРИКЛАДНАЯ МАТЕМАТИКА, Алгоритмы и методы наукоемкого программного обеспечения, утвержденной Ученым советом ФГАОУ ВО НИТУ "МИСиС" 22.09.2022, протокол № 8-22

Рабочая программа одобрена на заседании
Кафедра инженерной кибернетики

Протокол от 23.06.2021 г., №11

Руководитель подразделения Ефимов Альберт Рувимович

1. ЦЕЛИ ОСВОЕНИЯ	
1.1	Основная цель преподавания учебной дисциплины «Системы обеспечения информационной безопасности» – научить использовать современные технологии для реализации комплекса мер по защите информации в организации.
1.2	В рамках курса обучающийся должен изучить практики разработки и внедрения СОИБ организации в соответствии с государственными стандартами ГОСТ Р ИСО/МЭК 27000, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27005.

2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Блок ОП:	Б1.В.ДВ.08
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Введение в разработку приложений дополненной и виртуальной реальностей
2.1.2	Нейронные сети
2.1.3	Облачные технологии
2.1.4	Обработка естественного языка
2.1.5	Обучение с подкреплением
2.1.6	Программирование роботов II
2.1.7	Системный анализ и принятие решений
2.1.8	Системы автоматизированного проектирования
2.1.9	Экспертные и рекомендательные системы
2.1.10	Дискретные и нелинейные системы автоматического управления
2.1.11	Имитационное моделирование
2.1.12	Машинное обучение II
2.1.13	Методы и средства обработки изображений
2.1.14	Методы оптимизации
2.1.15	Основы мехатроники
2.1.16	Прикладной статистический анализ
2.1.17	Программирование роботов I
2.1.18	Производственная практика по освоению первичных навыков в области разработки наукоемкого ПО
2.1.19	Производственная практика по освоению первичных навыков в области разработки робототехнических и киберфизических систем
2.1.20	Фрактальный анализ
2.1.21	Математическое моделирование
2.1.22	Основы теории информации и автоматов
2.1.23	Основы электротехники и электроники
2.1.24	Современные технологии разработки мобильных приложений
2.1.25	Теория случайных процессов
2.1.26	Функциональный анализ
2.1.27	Численные методы
2.1.28	Безопасность жизнедеятельности
2.1.29	Операционные системы и среды
2.1.30	Основы теории информации и автоматов
2.1.31	Разработка клиент-серверных приложений
2.1.32	Сетевые технологии
2.1.33	Учебная практика по ознакомлению с технологиями разработки наукоемкого ПО
2.1.34	Учебная практика по ознакомлению с технологиями разработки робототехнических и киберфизических систем
2.1.35	Базы данных
2.1.36	Технологии программирования
2.1.37	Объектно-ориентированное программирование
2.1.38	Введение в специальность
2.1.39	Вычислительные машины, сети и системы
2.1.40	Программирование и алгоритмизация
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ
ПК-4: Способен выявлять естественно-научную сущность проблем, возникающих в ходе профессиональной деятельности, применять современный математический аппарат
Знать:
ПК-4-З1 Знать роль информации и связанные с ней процессы в области информационной безопасности.
УК-2: Способен собирать и интерпретировать данные и определять круг задач в рамках поставленной цели, выбирать оптимальные способы решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, умение обосновывать принятые решения
Знать:
УК-2-З1 Знать основные средства и продукты для защиты информации представленные на международном рынке.
ОПК-4: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности, разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения, выбирать и применять методики проектирования и актуальные инструментальные средства разработки
Знать:
ОПК-4-З1 Знать функциональные возможности серверных операционных систем реализующих безопасную и управляемую ИТ инфраструктуру.
УК-1: Способен осуществлять поиск, критический анализ и синтез информации, умение анализировать процессы и системы с использованием соответствующих аналитических, вычислительных и экспериментальных методов, применять системный подход для решения поставленных задач
Уметь:
УК-1-У1 Уметь обоснованно, комплексно, выбирать средства для обеспечения информационной безопасности.
ОПК-4: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности, разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения, выбирать и применять методики проектирования и актуальные инструментальные средства разработки
Уметь:
ОПК-4-У1 Уметь внедрять и использовать технологии серверных операционных систем для обеспечения безопасности организации.
УК-8: Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
Уметь:
УК-8-У1 Уметь работать с современным программным обеспечением реализующим принятые организацией меры по защите информации.
ОПК-4: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности, разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения, выбирать и применять методики проектирования и актуальные инструментальные средства разработки
Владеть:
ОПК-4-В1 Владеть навыком самостоятельного изучения и анализа технологических средств обеспечения информационной безопасности на предмет целесообразности их использования.

4. СТРУКТУРА И СОДЕРЖАНИЕ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Формируемые индикаторы компетенций	Литература и эл. ресурсы	Примечание	КМ	Выполняемые работы
	Раздел 1. Принципы защиты информации в компьютерных системах.							
1.1	Основные определения информационной безопасности и защиты информации. Регламентирующие организации. /Лек/	8	1	ПК-4-З1	Л1.1 Л1.2Л2.1 Л2.2 Э1			

1.2	Обзор основных нормативно-правовых актов и методических документов в области защиты информации. /Лек/	8	1	ПК-4-З1	Л1.1 Л1.2Л2.1 Л2.2 Э1			
1.3	Анализ рисков и проектирование политики безопасности организации. /Лек/	8	1	ПК-4-З1	Л1.1 Л1.2Л2.2 Э1			
1.4	Анализ рисков типовой организации. /Лаб/	8	2	ПК-4-З1	Л1.1 Л1.2Л2.1 Э1			
1.5	Создание политики безопасности типовой организации. /Лаб/	8	2	ПК-4-З1	Л1.1 Л1.2Л2.1 Э1			
1.6	Самостоятельная работа по материалам лекций и подготовка к контрольной работе Анализ рисков типовой организации. /Ср/	8	17	ПК-4-З1	Л1.1 Л1.2Л2.1 Э1			
1.7	Анализ рисков типовой организации. /Пр/	8	4	ПК-4-З1	Л1.1 Л1.2Л2.1 Э1			
1.8	Создание политики безопасности типовой организации. /Пр/	8	6	ПК-4-З1	Л1.1 Л1.2Л2.1 Э1			
	Раздел 2. Проектирование защищенной информационной структуры организации.							
2.1	Проведение анализа и самооценки безопасности организации. /Лек/	8	1	УК-1-У1 УК-2 -З1 УК-8-У1 ОПК-4-З1 ОПК-4-У1 ОПК-4-В1	Л1.1 Л1.2Л2.1 Э1			
2.2	Клиент-серверные антивирусы. Системы архивация и восстановление данных. Обеспечение бесперебойного питания /Лек/	8	1	УК-1-У1 УК-2 -З1 УК-8-У1 ОПК-4-З1 ОПК-4-У1 ОПК-4-В1	Л1.1 Л1.2Л2.1 Э1			
2.3	Служба каталогов Active Directory: установка, настройка. Управление пользователями и группами пользователей. Служба Active Directory облегченного доступа к каталогам. Система архивации данных Windows Server /Лек/	8	2	УК-1-У1 УК-2 -З1 УК-8-У1 ОПК-4-З1 ОПК-4-У1 ОПК-4-В1	Л1.1Л2.1 Э1			
2.4	Групповые политики Microsoft Window Server. Реализация конфигураций для пользователей и компьютеров. Параметры групповой политики содержатся в объектах групповой политики (GPO), которые связаны со следующими контейнерами службы каталогов Active Directory: сайты, домены и организационные единицы. /Лек/	8	1	УК-1-У1 УК-2 -З1 УК-8-У1 ОПК-4-З1 ОПК-4-У1 ОПК-4-В1	Л1.1Л2.1 Э1			

2.5	Примеры проектирования и использования Групповых политик для централизованного обеспечения защиты информации в организации. /Лек/	8	2	УК-1-У1 УК-2 -З1 УК-8-У1 ОПК-4-З1 ОПК-4-У1 ОПК-4-В1	Л1.1Л2.1 Э1			
2.6	Проектирование политики безопасности типовой организации. /Лаб/	8	4	УК-1-У1 УК-8 -У1 ОПК-4-З1 ОПК-4-У1 ОПК-4-В1	Л1.1Л2.1 Э1			
2.7	Проектирование профиля типовой организации. Настройка и установка типовой инфраструктуры организации: DNS, Active Directory, DHCP. /Лаб/	8	2	УК-1-У1 УК-8 -У1 ОПК-4-З1 ОПК-4-У1 ОПК-4-В1	Л1.1Л2.1 Э1			
2.8	Самостоятельная работа по материалам лекций. /Ср/	8	19	УК-1-У1 УК-2 -З1 УК-8-У1 ОПК-4-З1 ОПК-4-У1 ОПК-4-В1 ПК-4-З1	Л1.1 Л1.2Л2.1 Л2.2 Э1			
2.9	Проектирование политики безопасности типовой организации. /Пр/	8	6	ОПК-4-У1 ОПК-4-В1 УК-2-З1 УК-1-У1 ПК-4-З1	Л1.1 Л1.2Л2.1 Э1			
2.10	Проведение анализа и самооценки безопасности организации. /Пр/	8	4	ОПК-4-У1 ОПК-4-В1 УК-2-З1 УК-1-У1 ПК-4-З1	Л1.1 Л1.2Л2.1 Э1			
	Раздел 3. Применение технологий серверных операционных систем для обеспечения защиты информации в организации							
3.1	Службы политики сети и доступа. /Лек/	8	1	УК-1-У1 УК-2 -З1 УК-8-У1 ОПК-4-З1 ОПК-4-У1 ОПК-4-В1	Л1.1 Л1.2Л2.1 Э1			
3.2	Службы сертификатов Active Directory. /Лек/	8	1	УК-1-У1 УК-2 -З1 УК-8-У1 ОПК-4-З1 ОПК-4-У1 ОПК-4-В1	Л1.1Л2.1 Э1			
3.3	Реализация групповых политик для централизованного обеспечения защиты информации в организации /Лаб/	8	4	УК-1-У1 УК-8 -У1 ОПК-4-З1 ОПК-4-У1 ОПК-4-В1	Л1.1Л2.1 Э1			
3.4	Установка и настройка службы политики сети и доступа. /Лаб/	8	4	УК-1-У1 УК-8 -У1 ОПК-4-З1 ОПК-4-У1 ОПК-4-В1	Л1.1Л2.1 Э1			
3.5	Установка и настройка службы сертификатов Active Directory /Лаб/	8	6	УК-1-У1 УК-8 -У1 ОПК-4-З1 ОПК-4-У1 ОПК-4-В1	Л1.1Л2.1 Э1		КМ3	Р7

3.6	Самостоятельная работа по материалам лекций и подготовка к контрольной работе Разработка объектов групповой политики. /Ср/	8	12	УК-1-У1 УК-2-З1 УК-8-У1 ОПК-4-З1 ОПК-4-У1 ОПК-4-В1 ПК-4-З1	Л1.1Л2.1 Э1			
3.7	Реализация групповых политик для централизованного обеспечения защиты информации в организации /Пр/	8	4	ОПК-4-З1 ОПК-4-У1 ОПК-4-В1 УК-2-З1 ПК-4-З1	Л1.1Л2.1 Э1			

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

5.1. Контрольные мероприятия (контрольная работа, тест, коллоквиум, экзамен и т.п), вопросы для самостоятельной подготовки

Код КМ	Контрольное мероприятие	Проверяемые индикаторы компетенций	Вопросы для подготовки
КМ1	Контрольная работа №1. Защита информации в компьютерных системах.	УК-2-З1;ПК-4-З1	Основные определения информационной безопасности и защиты информации. Клиент-серверные антивирусы. Системы архивация и восстановление данных. Обеспечение бесперебойного питания. Шифрование данных.
КМ2	Контрольная работа №2. Проектирование защищённой информационной структуры организации.	ОПК-4-З1	Основные нормативно-правовые актовы и методические документы в области защиты информации. Регламентирующие организации. Проведение анализа и самооценки безопасности организации. Методология оценки безопасности информационных технологий. Методы и средства обеспечения безопасности. Методы менеджмента безопасности информационных технологий. Системы менеджмента информационной безопасности. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Менеджмент инцидентов информационной безопасности. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности. Выбор защитных мер. Анализ рисков при проектировании политики безопасности организации.
КМ3	Тест	ОПК-4-З1;УК-2-З1;ПК-4-З1	Основные определения информационной безопасности и защиты информации. Клиент-серверные антивирусы. Системы архивация и восстановление данных. Обеспечение бесперебойного питания. Шифрование данных. Основные нормативно-правовые актовы и методические документы в области защиты информации. Регламентирующие организации. Проведение анализа и самооценки безопасности организации. Методология оценки безопасности информационных технологий. Методы и средства обеспечения безопасности. Методы менеджмента безопасности информационных технологий. Системы менеджмента информационной безопасности. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Менеджмент инцидентов информационной безопасности. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности. Выбор защитных мер. Анализ рисков при проектировании политики безопасности организации.

5.2. Перечень работ, выполняемых по дисциплине (Курсовая работа, Курсовой проект, РГР, Реферат, ЛР, ПР и т.п.)			
Код работы	Название работы	Проверяемые индикаторы компетенций	Содержание работы
Р1	ЛР№1 Анализ рисков типовой организации.	ПК-4-З1	Анализ рисков типовой организации.
Р2	ЛР№2 Создание политики безопасности типовой организации.	ПК-4-З1	Проектирование политики безопасности типовой организации.
Р3	ЛР№3 Проектирование политики безопасности типовой организации.	ОПК-4-З1;ОПК-4-У1;ОПК-4-В1;УК-8-У1;УК-1-У1	Проектирование политики безопасности типовой организации.
Р4	ЛР№4 Проектирование профиля типовой организации. Настройка и установка типовой инфраструктуры организации: DNS, Active Directory, DHCP.	ОПК-4-З1;ОПК-4-У1;ОПК-4-В1;УК-8-У1;УК-1-У1	Проектирование профиля типовой организации. Настройка и установка типовой инфраструктуры организации: DNS, Active Directory, DHCP.
Р5	ЛР№5 Реализация групповых политик для централизованного обеспечения защиты информации в организации	ОПК-4-З1;ОПК-4-У1;ОПК-4-В1;УК-8-У1;УК-1-У1	Примеры реализации групповых политик Windows для централизованного обеспечения защиты информации в организации.
Р6	ЛР№6 Установка и настройка службы политики сети и доступа.	ОПК-4-З1;ОПК-4-У1;ОПК-4-В1;УК-8-У1;УК-1-У1	Установка и настройка службы политики сети и доступа.
Р7	ЛР№7 Установка и настройка службы сертификатов Active Directory	ОПК-4-З1;ОПК-4-У1;ОПК-4-В1;УК-8-У1;УК-1-У1	Установка и настройка службы сертификатов Active Directory.

5.3. Оценочные материалы, используемые для экзамена (описание билетов, тестов и т.п.)

Лабораторные работы №1 - №7

Контрольная работа №1 выполнение на лабораторном занятии.
Контрольная работа №2 выполнение на лабораторном занятии.

экзаменационный тест (тест проводится с использованием системы LMS Canvas).

5.4. Методика оценки освоения дисциплины (модуля, практики. НИР)

Шкала оценивания включает 4 уровня с оценками: отлично, хорошо, удовлетворительно, неудовлетворительно.

Критерии оценивания выполнения лабораторных работ.
Лабораторная работа считается выполненной если:
Даны исчерпывающие и обоснованные ответы на все поставленные вопросы, задание выполненное на компьютере не содержит ошибок.

Критерии оценивания контрольных работ
Оценка «неудовлетворительно» – выставляется в случае, если: работа не соответствует заданию, выполнена не полностью.
Оценка «отлично», «хорошо», «удовлетворительно» – зависит от сложности поставленной задачи. Выполненная работа не содержит ошибок, соответствует заданию.

Критерии оценивания тестов
Критерии выставления оценок за тест, состоящий 25 вопросов.
Время выполнения работы: 45 мин.
Оценка «отлично» – 90% правильных ответов;
Оценка «хорошо» – 80% правильных ответов;
Оценка «удовлетворительно» – 70% правильных ответов;
Оценка «неудовлетворительно» – ниже 70% правильных ответов.

Итоговая оценка по курсу вычисляется как среднее арифметическое оценок за КР-1, КР-2, Тест-1 при условии выполнения и защиты лабораторных работ.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л1.1	Пакин А. И.	Информационная безопасность информационных систем управления предприятием: учебное пособие	Электронная библиотека	Москва: Альтаир|МГАВТ, 2009
Л1.2	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Электронная библиотека	Самара: Самарский государственный архитектурно-строительный университет, 2014

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л2.1	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Электронная библиотека	Москва, Берлин: Директ-Медиа, 2020
Л2.2	Костин В. Н.	Методы и средства защиты компьютерной информации. Информационная безопасность компьютерных сетей (N 3085): учеб. пособие	Электронная библиотека	М.: [МИСиС], 2018

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Э1		https://fstec.ru/

6.3 Перечень программного обеспечения

П.1	Лицензии ПО Windows Server CAL ALNG LicSAPk MVL DvcCAL, ПО WinEDUA3 ALNG SubsVL MVL PerUsr и PerUsr

6.4. Перечень информационных справочных систем и профессиональных баз данных

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Ауд.	Назначение	Оснащение

Б-904а	Учебная аудитория:	20 стационарных компьютеров (core i5-3470 8gb RAM), пакет лицензионных программ MS Office, демонстрационное оборудование: доска, проектор мультимедийный, экран, колонки, комплект учебной мебели
Б-902	Учебная аудитория:	12 стационарных компьютеров (2 x core i5-3470 8gb RAM, 10 x ryzen5 2400g 32gb RAM), пакет лицензионных программ MS Office, демонстрационное оборудование: доска, проектор мультимедийный, комплект учебной мебели
Б-907	Учебная аудитория:	1 стационарный компьютер, пакет лицензионных программ MS Office, комплект учебной мебели на 42 посадочных места, демонстрационное оборудование: доска, проектор мультимедийный x 2, экран x 2, колонки
Читальный зал электронных ресурсов		комплект учебной мебели на 55 мест для обучающихся, 50 ПК с доступом к ИТС «Интернет», ЭИОС университета через личный кабинет на платформе LMS Canvas, лицензионные программы MS Office, MS Teams, ESET Antivirus.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

Освоение дисциплины требует значительного объема самостоятельной работы. Отдельные учебные вопросы выносятся на самостоятельную проработку и контролируются посредством текущей аттестации. При этом организуются групповые и индивидуальные консультации.

Качественное освоение дисциплины возможно только при систематической самостоятельной работе, что поддерживается защитой лабораторных работ.

Самостоятельная работа обучающихся направлена на углубленное изучение тем дисциплины и предполагает изучение основных и дополнительных источников учебной и научной литературы. Полученные знания и навыки в дальнейшем будут использованы при выполнении студенческих научных исследований и стать основой для выступления на студенческих научно-практических конференциях, конкурсах студенческих работ, при подготовке ВКР и пр.