МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Рабочая программа дисциплины (модуля)

Информационная безопасность

Закреплена за подразделением Кафедра АСУ

Направление подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Профиль

Квалификация **Бакалавр**
Форма обучения **очная**
Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 51
самостоятельная работа 22
часов на контроль 35

Формы контроля в семестрах:
экзамен 4

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**4 (2.2)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	17	17	17	17
Лабораторные	17	17	17	17
Практические	17	17	17	17
Итого ауд.	51	51	51	51
Контактная работа	51	51	51	51
Сам. работа	22	22	22	22
Часы на контроль	35	35	35	35
Итого	108	108	108	108

Программу составил(и):
-, ст.преп., Агабубаев Аслан Такабудинович

Рабочая программа
Информационная безопасность

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 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА (приказ от 02.04.2021 г. № 119 о.в.)

Составлена на основании учебного плана:

09.03.01 Информатика и вычислительная техника, 09.03.01-БИВТ-22.plx , утвержденного Ученым советом ФГАОУ ВО НИТУ "МИСиС" в составе соответствующей ОПОП ВО 22.09.2022, протокол № 8-22

Утверждена в составе ОПОП ВО:

09.03.01 Информатика и вычислительная техника, , утвержденной Ученым советом ФГАОУ ВО НИТУ "МИСиС" 22.09.2022, протокол № 8-22

Рабочая программа одобрена на заседании
Кафедра АСУ

Протокол от 05.07.2022 г., №10

Руководитель подразделения Темкин Игорь Олегович

1. ЦЕЛИ ОСВОЕНИЯ	
1.1	формирование у обучающихся профессиональных компетенций в области защиты данных и безопасности IT-инфраструктуры предприятия.

2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ		
Блок ОП:		Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**	
2.1.1	Объектно-ориентированное программирование	
2.1.2	Программирование и алгоритмизация	
2.1.3	Технологии программирования	
2.1.4	Базы данных	
2.1.5	Вычислительные машины, сети и системы	
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**	
2.2.1	Подготовка к процедуре защиты и защита выпускной квалификационной работы	
2.2.2	Защита информации	
2.2.3	Геоинформационные платформы	
2.2.4	Проектирование систем управления взаимодействием распределенных объектов	
2.2.5	Производственная практика	

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Знать:
ОПК-3-З1 сущность и значение информации в развитии современного общества. основные закономерности функционирования информационных процессов в различных системах
ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности
Знать:
ОПК-2-З1 принципы и методы поиска, анализа и синтеза информации. аналитические, вычислительные и экспериментальные методы анализа
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Уметь:
ОПК-3-У1 применять системный подход к решению поставленных профессиональных задач. обрабатывать запросы и управлять процессами системы
ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности
Уметь:
ОПК-2-У1 использовать базовые знания об информационных системах для решения прикладных задач защиты информации
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Владеть:
ОПК-3-В1 практическими навыками поиска, анализа и синтеза информации. методами описания процессов и построения систем
ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности
Владеть:
ОПК-2-В1 навыками использование программных инструментов в задачах защиты информации

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. Обеспечение информационной безопасности и принципы кодирования							
1.1	Основные понятия и определения /Лек/	4	3	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-З1	Л1.1 Л1.2 Э1			
1.2	Настройка сетевой инфраструктуры предприятия. HCIA-Security Training /Лаб/	4	5	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-З1	Л1.1 Л1.2Л2.1			
1.3	Нормативно-правовая база функционирования систем защиты информации /Ср/	4	5	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-З1	Л1.1 Л1.2Л3.1 Э1			
1.4	Источники, риски и формы атак на информацию /Лек/	4	2	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-З1	Л1.1 Л1.2			
1.5	Политика безопасности. Стандарты безопасности /Лек/	4	2	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-З1	Л1.1 Л1.2			
1.6	Построение сетевой безопасности. HCIA /Лаб/	4	6	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-З1	Л1.1 Л1.2Л2.1			
1.7	Меры по обеспечению сохранности информации и угрозы ее безопасности /Ср/	4	5	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-З1	Л1.1 Л1.2Л3.1			
1.8	Модели безопасности ОС /Лек/	4	2	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-З1	Л1.1 Л1.2			
1.9	Настройка безопасности. Прикладной уровень /Лаб/	4	6	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-З1	Л1.1 Л1.2Л2.1 Э1			

1.10	Способы встраивания защитных механизмов в программное обеспечение /Ср/	4	5	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-З1	Л1.1 Л1.2Л3.1			
1.11	Алгоритмы аутентификации пользователей /Лек/	4	2	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-З1	Л1.1 Л1.2 Э1			
1.12	Администрирование сетей /Лек/	4	2	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-З1	Л1.1 Л1.2			
1.13	Многоуровневая защита корпоративных сетей, защита информации в сетях /Лек/	4	2	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-З1	Л1.1 Л1.2			
1.14	Требования к системам защиты информации /Лек/	4	2	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-З1	Л1.1 Л1.2			
1.15	требования к составу проектной и эксплуатационной документации систем информационной защиты /Ср/	4	7	ОПК-3-З1 ОПК-3-У1 ОПК-3-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-З1	Л1.1 Л1.2Л3.1			
1.16	Базовые концепции организации сетей и основные сетевые устройства /Пр/	4	2		Э2			Р2
1.17	Обзор основных операционных систем /Пр/	4	2					Р2
1.18	Сетевые экраны и антивирусное обеспечение для операционных систем /Пр/	4	2					Р2
1.19	Построение отказоустойчивых межсетевых экранов /Пр/	4	2					Р2
1.20	Управление пользователями на межсетевых экранах Huawei /Пр/	4	2					Р2
1.21	Анализ направлений передачи информации /Пр/	4	4					Р2
1.22	Экстренная реакция на вторжение /Пр/	4	3					Р2

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	Экзамен	ОПК-3-31;ОПК-2-31	Обзор информационной безопасности 1.Базовые сетевые концепции Архитектура сетей TCP/IP Распространенные сетевые протоколы 2.Стандарты и рекомендации Стандарты информационной безопасности ISO 27001 ISMS 3.Распространенные сетевые устройства Базовые сетевые устройства Первичный вход на устройство 4.Тенденции развития защиты от угроз и информационной безопасности Защита от угроз Тенденции развития информационной безопасности 5.Распространенные угрозы информационной безопасности Обзор текущей ситуации Безопасность приложений 6.Основные понятия информационной безопасности Риски и активы Анализ защищенности 1.Аварийное реагирование на инцидент безопасности Обзор Процесс реагирования на инцидент безопасности 2.Мониторинг и анализ данных Проактивный анализ Пассивный сбор данных Анализ данных 4.Цифровая криминалистика Киберпреступность Обзор цифровой криминалистики Процесс криминластики 5.Рекомендации и лучшие практики, разбор сценариев Процедура развертывания системы безопасности Распространенные сценарии Основы сетевой безопасности 1.Управление пользователями МСЭ Пользовательская аутентификация и сервисы AAA Управление процессом аутентификации 2.Обзор IPS Обзор систем предотвращения вторжений Обзор сетевого антивируса 3.Введение в межсетевые кэраны Обзор МСЭ Политики инспектирования ASPF 4.Резервирование Dual-System Hot Standby 5.Network Address Translation Принципы трансляции сетевых адресов NAT Source NAT

			Безопасность ОС и хостов 1.Хостовые МСЭ и антивирусное ПО Windows Firewalls Linux Firewalls Антивирусное ПО 2.Обзор операционной системы Operating System 101 Windows Operating System Linux Operating System 3.Распространенные типы серверов и угроз Обзор серверных платформ Серверное ПО Распространенные атаки и уязвимости Сервисы шифрования 1.Public Key Infrastructure (PKI) Certificate System Цифровые сертификаты Структура PKI 2.Механизмы криптографии Основы криптографии Обзор VPN Настройка VPN 3.Шифрование и дешифрование Алгоритмы шифрования Распространенные современные алгоритмы

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	Лабораторные занятия	ОПК-3-У1;ОПК-3-В1;ОПК-2-У1;ОПК-2-В1	Введение в межсетевые экраны Технология NAT Построение отказоустойчивых межсетевых экранов Управление пользователями на межсетевых экранах Huawei Введение в системы предотвращения вторжения Криптография
Р2	Практические занятия	ОПК-3-У1;ОПК-3-В1;ОПК-2-У1;ОПК-2-В1	Основные механизмы шифрования Инфраструктура открытых ключей Применение криптографии для обеспечения информационной безопасности Планирование информационной безопасности Анализ направлений передачи информации Цифровая криминалистика Экстренная реакция на вторжение

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

Экзаменационный билет состоит из двух теоретических вопросов. Билеты хранятся на кафедре.

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

В рамках освоения дисциплины студент обязан выполнить все виды лабораторных работ, выполнение которых определяет допуск к экзамену для сдачи теоретической части дисциплины.
Дисциплина считается освоенной при выполнении следующих условий:
- текущий лекционный контроль имеет положительные оценки ("удовлетворительно"; "хорошо"; "отлично");
- выполнены и защищены все лабораторные работы;
- промежуточное и итоговое тестирование выполнено с результатами:
от 25 и менее 50 % – «удовлетворительно;
от 50 и менее 75 % – «хорошо»;
от 75 до 100 % – «отлично».

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

6.1. Рекомендуемая литература

6.1.1. Основная литература				
	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л1.1	Рытенкова О.	Информационная безопасность: журнал	Электронная библиотека	Москва: ГРОТЕК, 2012
Л1.2	Рытенкова О.	Информационная безопасность: журнал	Электронная библиотека	Москва: ГРОТЕК, 2013
6.1.2. Дополнительная литература				
	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л2.1	Ниссенбаум О. В.	Теоретико-числовые методы в криптографии. Сборник заданий: учебно-методическое пособие для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем», направления «Информационная безопасность»: учебно-методическое пособие	Электронная библиотека	Тюмень: Тюменский государственный университет, 2014
6.1.3. Методические разработки				
	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л3.1	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Электронная библиотека	Москва, Берлин: Директ-Медиа, 2020
6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э1	Электронная система НИТУ МИСиС -LMS Canvas	https://lms.misis.ru/		
Э2	HCIA	https://ilearningx.huawei.com/portal/courses/HuaweiX+EBGTC00000471/about		
6.3 Перечень программного обеспечения				
П.1	Microsoft Office			
П.2	LMS Canvas			
П.3	MS Teams			
6.4. Перечень информационных справочных систем и профессиональных баз данных				
И.1	Scopus - единая реферативная база данных научных публикаций (www.scopus.com)			
И.2	Единое окно доступа к образовательным ресурсам (http://window.edu.ru)			
И.3	ScienceDirect - база полнотекстовых научных журналов и книг издательства Эльзевир (www.sciencedirect.com)			

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ		
Ауд.	Назначение	Оснащение
Л-826	Учебная аудитория:	доска и маркеры, персональные компьютеры ОС Windows с администраторскими правами доступа, с проводными сетевыми платами, с COM-портами количеством не менее 6, сетевое коммуникационное оборудование CISCO: 6 коммутаторов и 6 маршрутизаторов, обжатые кабели витая пара прямые и кроссовые количеством не менее 12 каждый, консольные кабели количеством не менее 6.
Любой корпус Мультимедийная	Учебная аудитория для проведения занятий лекционного типа и/или для проведения практических занятий:	комплект учебной мебели до 36 мест для обучающихся, мультимедийное оборудование, магнитно-маркерная доска, рабочее место преподавателя, ПКс доступом к ИТС «Интернет», ЭИОС университета через личный кабинет на платформе LMS Canvas, лицензионные программы MS Office, MS Teams, ESET Antivirus

Читальный зал №3 (Б)		комплект учебной мебели на 44 места для обучающихся, МФУ Xerox VersaLink B7025 с функцией масштабирования текстов и изображений, 8 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

Подготовка к лекциям.
Подготовка к лекционному занятию включает выполнение всех видов заданий, рекомендованных к каждой лекции, т.е. задания выполняются еще до лекционного занятия по соответствующей теме.
В ходе лекционных занятий необходимо вести конспектирование учебного материала, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. При необходимости задавать преподавателю уточняющие вопросы.
Работая над конспектом лекций, Вам всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.
Подготовку к каждому лабораторному занятию Вы должны начать с ознакомления с планом лабораторного занятия, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, рекомендованной к данной теме. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.
В процессе подготовки к лабораторным занятиям, Вам необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы. При всей полноте конспектирования лекции в ней невозможно изложить весь материал из-за лимита аудиторных часов. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у Вас отношение к конкретной проблеме.
Ваша самостоятельная работа может осуществляться в аудиторной и внеаудиторной формах. Самостоятельная работа в аудиторное время включает:
Самостоятельную работу по теоретическому курсу: аудиторную самостоятельную работу на лекциях, работу с лекционным материалом после лекции, выполнение дополнительных индивидуальных заданий на лабораторных работах.
Самостоятельная работа на лекции выполняется в конце каждой лекции и заключается в решении небольшой задачи, поставленной преподавателем по материалу прочитанной лекции.
Работа с лекцией включает в себя дополнение конспекта сведениями из рекомендованной литературы (с указанием использованного источника).
Возможны выступления обучающихся на лекции по отдельным вопросам обсуждаемой темы (проработанные самостоятельно под руководством преподавателя); сообщения занимают 7…10 мин. Такие выступления помогают четко выражать свои мысли, аргументировано излагать и отстаивать свою точку зрения при ответе на вопросы. Самостоятельное изучение практического материала планируется из расчета 0,3 ч на 1 ч лекции.
Работа с материалом лекции, выполненная через один-два дня после ее прослушивания, позволяет выделить неясные моменты, которые необходимо либо самостоятельно разобрать, пользуясь рекомендованными литературными источниками, либо обсудить с преподавателем на ближайшей консультации.
Внеаудиторную самостоятельную работу. Перечень лабораторных работ, а также список учебных и методических пособий для этих работ вывешивается в лаборатории и студенты имеют возможность подготовиться к выполнению этих работ.
Используется лабораторный практикум "Разработка автоматизированных экспертных систем". Внеаудиторная самостоятельная работа по лабораторным занятиям включает подготовку к выполнению работ, обработку полученных результатов, защиту работ.
Подготовка заключается в ознакомлении с названием, целью работы, основными теоретическими положениями и методическими указаниями по ее выполнению.