МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Рабочая программа дисциплины (модуля)

Защита информации

Закреплена за кафедрой		Базовых дисциплин
Направление подготовки		27.03.04 Управление в технических системах
Профиль		Информационные технологии в управлении
Квалификация	**Бакалавр**	
Форма обучения	**очная**	
Общая трудоемкость	**3 ЗЕТ**	
Часов по учебному плану	108	Формы контроля в семестрах:
в том числе:		зачет с оценкой 8
аудиторные занятия	36	
самостоятельная работа	70	

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	14			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Практические	18	18	18	18
Контроль самостоятельной работы	2	2	2	2
В том числе в форме практ.подготовки	14		14	
Итого ауд.	36	36	36	36
Контактная работа	38	38	38	38
Сам. работа	70	70	70	70
Итого	108	108	108	108

Программу составил(и):

ктн, Доц., Уснунц-Кригер Татьяна Николаевна

_____

_____

Рабочая программа

Защита информации

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 27.03.04 Управление в технических системах (приказ от 02.04.2021 г. № 119 о.в.)

Составлена на основании учебного плана:

27.03.04 Управление в технических системах, УТС-25.plx Информационные технологии в управлении, утвержденного Ученым советом ВФ НИТУ "МИСиС" 26.12.2024, протокол № 4-24

Рабочая программа одобрена на заседании кафедры

Базовых дисциплин

Протокол от 14.05.2025 г., №9

Зав. кафедрой Уснунц-Кригер Т.Н. _____

1. ЦЕЛИ ОСВОЕНИЯ	
1.1	Целями освоения учебной дисциплины "Защита информации" являются,изучение организационных, технических, алгоритмических и других методов и средств защиты компьютерной информации, - законодательства и стандартов в этой области, - современных криптосистем, -методов борьбы с вирусами для последующего применения в учебной и практической деятельности.
1.2	

2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Интернет-технологии
2.1.2	Защита интеллектуальной собственности
2.1.3	Методы цифровой обработки
2.1.4	Математика
2.1.5	Вычислительные машины, системы и сети
2.1.6	Информатика
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Технологическая (производственно-технологическая) практика
2.2.2	Выполнение, подготовка к процедуре защиты и защита выпускной квалификационной работы
2.2.3	Преддипломная практика

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ
ПК-1: Способен осуществлять обработку научно-технической информации и результатов исследований
ПК-1.2: Владеет методами исследования с дальнейшей обработкой полученной информации, интерпретирует результаты и делает выводы
Знать:
ПК-1.2-З1 нормативные документы в области защиты информации
ПК-1.2-З2 критерии оценки обеспечения информационной безопасности в соответствии с действующими нормативноправовыми документами в своей профессиональной деятельности
Уметь:
ПК-1.2-У1 использовать нормативные документы в области защиты информации
ПК-1.2-У2 использовать нормативные документы в своей профессиональной деятельности
ПК-1.2-У3 использовать навыки работы с компьютером, соблюдать основные требования информационной безопасности
Владеть:
ПК-1.2-В1 навыками работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература и эл. ресурсы	Примечание
	Раздел 1. Основные понятия					
1.1	Основные понятия и определения ИБ и ЗИ /Лек/	8	2	ПК-1.2	Л1.1 Э1 Э2	
1.2	Актуальность проблемы обеспечения безопасности информации в технических ситемах /Лек/	8	3	ПК-1.2	Л1.1 Э1 Э2	
1.3	Освоение лекционного материала с использованием конспекта, презентации и рекомендуемой литературы. /Ср/	8	10	ПК-1.2	Л1.1 Э1 Э2	
	Раздел 2. Законодательные и правовые основы защиты компьютерной информации информационных					

2.1	Законодательные и правовые основы защиты компьютерной информации информационных технологий /Лек/	8	3	ПК-1.2	Л1.1 Э1 Э2	
2.2	Подготовка к выполнению: Домашнее задание №1 -"Концептуальные основы и организационно-правовые аспекты ЗИ". /Пр/	8	4	ПК-1.2	Л1.1 Э1 Э2	
2.3	Освоение лекционного материала с использованием конспекта, презентации и рекомендуемой литературы.Выполнение ДЗ-1. /Ср/	8	10	ПК-1.2	Л1.1 Э1 Э2	
	Раздел 3. Угрозы информации; виды возможных нарушений информационной системы					
3.1	Угрозы информации; виды возможных нарушений информационной системы /Лек/	8	2	ПК-1.2	Л1.1 Э1 Э2	
3.2	Подготовка к выполнению:Контрольная работа №1-"Классификация угроз.Виды нарушений информационной системы". /Пр/	8	4	ПК-1.2	Л1.1 Э1 Э2	
3.3	Освоение лекционного материала с использованием конспекта, презентации и рекомендуемой литературы.Выполнение Контрольной работы № 1. /Ср/	8	10	ПК-1.2	Л1.1 Э1 Э2	
	Раздел 4. Теоретические основы компьютерной безопасности					
4.1	Теоретические основы компьютерной безопасности. /Лек/	8	2	ПК-1.2	Л1.1 Э1 Э2	
4.2	Подготовка к выполнению: Домашнее задание №2 -"Проектирование информационного ресурса по ИБ. Часть 1". /Пр/	8	4	ПК-1.2	Л1.1 Э1 Э2	
4.3	Освоение лекционного материала с использованием конспекта, презентации и рекомендуемой литературы.Выполнение ДЗ-2. /Ср/	8	10	ПК-1.2	Л1.1 Э1 Э2	
	Раздел 5. Современные криптосистемы для защиты компьютерной информации					
5.1	Современные криптографические модели. Алгоритмы шифрования. /Лек/	8	2	ПК-1.2	Л1.1 Э1 Э2	
5.2	Подготовка к выполнению:Контрольная работа №2 -"Математические основы криптографических методов" /Пр/	8	3	ПК-1.2	Л1.1 Э1 Э2	
5.3	Проработка лекционного материала. Самостоятельное изучение литературы. Самостоятельное изучение рекомендованных открытых источников. /Ср/	8	15	ПК-1.2	Л1.1 Э1 Э2	
	Раздел 6. Политика безопасности предприятий					
6.1	Политика безопасности предприятий. Стандарты безопасноти. /Лек/	8	2	ПК-1.2	Л1.1 Э1 Э2	
6.2	Алгоритмы аутентификации пользователей /Лек/	8	2	ПК-1.2	Л1.1 Э1 Э2	
6.3	Проектирование информационного ресурса по ИБ. Часть 2. /Пр/	8	3	ПК-1.2	Л1.1 Э1 Э2	
6.4	Освоение лекционного материала с использованием конспекта, презентации и рекомендуемой литературы. /Ср/	8	15	ПК-1.2	Л1.1 Э1 Э2	

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

5.1. Вопросы для самостоятельной подготовки к экзамену (зачёту с оценкой)

Вопросы к зачету с оценкой:

1. Основные принципы защиты информационных технологий (четыре задачи системы защиты)
2. Виды угроз собственной информации в сфере финансовой деятельности
3. Меры противодействия угрозам собственной информации

4. Организационно-технические меры защиты информации посредством: охраны зданий; организации использования оргтехники; контроля за посетителями, клиентами.
5. Организационные меры защиты информации посредством контроля за сотрудниками.
6. Организация защиты конфиденциальных документов.
7. Информационная безопасность при использовании средств связи.
8. Организационно-технические методы получения информации о конкурентах.
9. Понятие «изъяны защиты». Причины существования изъянов защиты.
10. Классификация изъянов защиты (по источнику появления, по этапам внедрения, по размещению в информационной системе).
11. Таксономия причин возникновения изъянов защиты;
12. Понятие политики безопасност;.
13. Дискретные модели безопасности;
14. Мандатные модели безопасности;
15. Ролевые модели безопасности;
16. Понятия идентификация, аутентификация.Методы и типы аутентификации;
17. Парольные системы защиты;
18. Понятие шифрования. Виды шифрования, применяемые в информационных системах. 19. Способы контроля целостности данных.
20. Цифровая подпись.
21. Хэш-функция.
22. Компьютерная стеганография.
23. Классификация нарушителей по уровню возможностей.
24. Пароль - как метод защиты информации. Виды паролей. Правила подбора паролей.
25. Классификация мероприятий по защите от несанкционированного доступа.
26. Охарактеризовать область физической безопасности АС.
27. Охарактеризовать область безопасности персонала.
28. Охарактеризовать область безопасности оборудования.
29. Охарактеризовать область безопасности ПО.
30. Межсетевые экраны – как метод защиты информации. Дать определение МЭ.
31. Инспектирование и анализ протоколов - как метод защиты информации.
32. Контроль за действиями пользователя и событиями в сети.
33. Принципы восстановления информации и защиты после аварии.
34. Хранение информации. Сжатие и защита информации при хранении.
35. Современные программные угрозы, методы их обнаружения и предупреждения.
36. Методы обнаружения разрушающих программных средств.
37. Намеренное силовое воздействие по каналу связи - как угроза безопасности АС.

5.2. Перечень работ, выполняемых по дисциплине (модулю, практике, НИР) - эссе, рефераты, практические и расчетно-графические работы, курсовые работы, проекты и др.

По дисциплине предусмотрено выполнение домашних заданий, контрольных мероприятий, направленных на контроль компетенций:
Домашнее задание ДЗ-1: Концептуальные основы и организационно-правовые аспекты ЗИ;
Домашнее задание ДЗ-2: Проектирование информационного ресурса по ИБ;

Контрольная работа №1: Классификация угроз.Виды нарушений информационной системы;
Контрольная работа №2: Математические основы криптографических методов.

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

По дисциплине не предусмотрен экзамен.

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

ШКАЛА ОЦЕНИВАНИЯ ДОМАШНИХ ЗАДАНИЙ:
Оценка "зачтено" - задания выполнены полностью, расчеты выполнены верно, технически грамотно оформлены.
Оценка "не зачтено" - задания выполнены не в полном объёме, допущены ошибки в расчете и имеются недочеты в оформлении заданий.
Промежуточная аттестация по дисциплине предусмотрена в форме зачета с оценкой.

ШКАЛА ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ:
а) "отлично"-студент показывает глубокие, исчерпывающие знания в обьеме пройденнй программы, уверенно действует по применению полученных знаний на практике, грамотно и логически стройно излагает материал при ответе, умеет формулировать выводы из изложенного теоретического материала, знает дополнительную литературу;
б) "хорошо"-студент показывает твердые и достаточно полные знания в обьеме пройденной программы, допускает незначительные ошибки при освещении заданных вопросов, правильно действует по применению на практике. четко излагает материал;
в) "удовлетворительно"-студент показывет знания в обьеме пройденной программы, ответы излагает хотя и с ошибками, но уверенно исправляемымым после дополнительных и наводящих вопросов, правильно действует по применению знаний на практике;
г) "неудовлетворительно"-студент допускает грубые ошибки в ответе, не понимает сущности излагаемого вопроса, не умеет применять знания на практике, дает неполные ответы на дополнительные и наводящие вопросы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л1.1	Громов Ю.Ю. Громов Ю.Ю.,Драчев В.О.,Иванов О.Г., Шахов Н.Г.	Основы информационной безопасности: учебное пособие	Электронный каталог	Старый Оскол ТНТ, 2017

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Э1	Защита информации - Электронная библиотечная система(ЭБС)	https://lms.misis.ru/
Э2	Защита информации - ООО" НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА"	http://elibrary.misis.ru/action.php?kt_path_info=ktcore.SecViewPlugin.actions.document&fDocumentId=12459

6.3 Перечень программного обеспечения

П.1	MS Office
П.2	MS Teams

6.4. Перечень информационных справочных систем и профессиональных баз данных

И.1	Научная электронная библиотека eLIBRARY.ru – URL: https://elibrary.ru/
И.2	Научная электронная библиотека МИСиС - URL: http://elibrary.misis.ru/login.php
И.3	Электронная библиотечная система (ЭБС) – «Университетская библиотека онлайн» открытый круглосуточный доступ через интернет с регистрацией в библиотеке и вводом пароля.- URL: http://biblioclub.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Ауд.	Назначение	Оснащение
4	Защита информации	компьютер, проектор, экран, интерактивная доска комплект тематических презентаций, доступ к

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

Весь курс разделен на самостоятельные взаимосвязанные части, т.е. имеет модульное построение. Развитие самостоятельности студентов достигается индивидуализацией домашних заданий и вопросов для внутрисеместрового контроля знаний. Это обеспечивается методическими разработками, существенно повышающими эффективность самостоятельной работы студентов.

Лекции проводятся с использованием мультимедийных технологий в специально оборудованных аудиториях, при этом лекционный материал демонстрируется с использованием графического редактора Power Point.

На практических занятиях и при выполнении домашних занятий осваиваются, как классические методы решения задач, так и с использованием пакетов прикладных программ. Такая возможность обеспечивается рациональным использованием времени при проведении лекций и практических занятий с широким привлечением мультимедийной техники, и современных пакетов прикладных программ, а также формированием требований к подготовке студентов по предшествующим дисциплинам (математика, информатика, физика и др.) Отдельные учебные вопросы выносятся на самостоятельную проработку и контролируются посредством текущей аттестации. При этом организуются групповые и индивидуальные консультации.