

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
СТАРООСКОЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ ИМ. А.А. УГАРОВА
 (филиал) федерального государственного автономного образовательного учреждения
 высшего образования
 «Национальный исследовательский технологический университет «МИСИС»
СТИ НИТУ «МИСИС»

Рабочая программа утверждена
 решением Ученого совета
 СТИ НИТУ «МИСИС»
 от «23» июня 2026 г.
 протокол № 38

Рабочая программа дисциплины

Информационная безопасность

Кафедра автоматизированных и информационных систем управления им.

Закреплена за кафедрой Ю.И.Еременко
 Направление подготовки 09.03.02 Информационные системы и технологии
 Профиль Информационные системы и технологии
 Квалификация Бакалавр
 Форма обучения Очная
 Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану	144
в том числе:	
аудиторные занятия	51
самостоятельная работа	57
часов на контроль	36

Формы контроля в семестрах:
 экзамен 7, курсовая работа 8

Распределение часов дисциплины по семестрам

Семестр	7		8		Итого	
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	17	17	-	-	17	17
Лабораторные	17	17	-	-	17	17
Практические	17	17	-	-	17	17
Контактная работа	51	51	-	-	51	51
Сам. работа	21	21	36	36	57	57
Часы на контроль	36	36	-	-	36	36
Итого	108	108	36	36	144	144

Год набора 2026 г.

Программу составил:
доцент каф. АИСУ, кандидат технических наук
Соловьев Антон Юрьевич



Должность, уч. ст., уч. зв. ФИО полностью

подпись

Рабочая программа дисциплины

Информационная безопасность

наименование

Разработана в соответствии с ОС ВО НИТУ «МИСиС»:

Самостоятельно устанавливаемый образовательный стандарт высшего образования – бакалавриат
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский технологический университет «МИСиС» по направлению подготовки
09.03.02 Информационные системы и технологии (приказ от 05.03.2020 г. № 95 о.в.)

Составлена на основании учебного плана 2026 год набора по направлению подготовки

09.03.02. Информационные системы и технологии,

Профиль: *Информационные системы и технологии*, утвержденного Ученым советом СТИ НИТУ "МИСИС" ,
протокол №38 от 23.06.2026 г.

Рабочая программа одобрена на заседании кафедры Автоматизированных и информационных систем
управления им. Ю.И.Еременко

Протокол от «22» июня 2026 г. № 6

И.о. зав. кафедрой АИСУ
аббревиатура наименования кафедры



подпись

Д.А. Полещенко
И.О. Фамилия

«22» июня 2026 г.

Руководитель ОПОП ВО
И.о. зав. каф. АИСУ, кандидат технических наук,
доцент



подпись

Д.А. Полещенко
И.О. Фамилия

22.06.2026

1. ЦЕЛИ ОСВОЕНИЯ	
Цель дисциплины – формирование теоретических знаний в области управления информационными ресурсами систем и сетей и отработка умений и навыков использования инструментальных программных систем, сетевых служб и оборудования для защиты информации в компьютерных системах.	
Задачи дисциплины:	
• Научить обучающихся основным терминам и понятиям защиты информации; • Научить обучающихся применять теоретические знания в области защиты информации для решения конкретных практических задач по выбранному направлению подготовки; • Научить обучающихся основным угрозам защиты информации и способам их предотвращения; • Научить обучающихся разбираться в типовых атаках направленных на ИС и программные продукты; • Научить обучающихся основным видам криптографических алгоритмов и их уязвимостей	

2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Часть ОПОП ВО	Б1.О
2.1	Требования к предварительной подготовке обучающихся – предшествующие дисциплины
2.1.1	Математика
2.1.2	Информатика
2.1.3	Правовые основы профессиональной деятельности
2.2	Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее:
2.2.1	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

УК-1; ОПК-2; ОПК-3; ПК-1

3. ИНДИКАТОРЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ, СОВМЕЩЕННЫЕ С РЕЗУЛЬТАТАМИ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ	
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	
Знать:	УК-1-31– Знать основные понятия и термины, связанные с информационной безопасностью; УК-1-32 –Знать основные виды угроз информационной безопасности;
Уметь:	УК-1-У1 – Уметь определять и классифицировать угрозы и атаки.
Владеть:	УК-1-В1 – Владеть навыками обнаружения уязвимостей веб-ресурсов
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-3-31– Знать нормативную и законодательную базу в области информационной безопасности
Уметь:	ОПК-3-У1 – Уметь проводить анализ защищенности информационных объектов в различных сферах деятельности человека;
Владеть:	ОПК-3-В1– Владеть навыками реализации поиска потенциально компрометирующей информации в интернете
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-2-31– Знать современное программное обеспечение для защиты информации
Уметь:	ОПК-2-У1 – Уметь проводить анализ работы программ защиты информации
Владеть:	ОПК-2-В1– Владеть навыками развертывания систем защиты информации

ПК-1 Способен участвовать в работах по: - доводке и освоению информационных технологий в ходе внедрения и эксплуатации информационных технологий; - поддержанию работоспособности информационных систем и технологий в заданных функциональных характеристиках и в соответствии с критериями качества; - управлению программно-аппаратными средствами информационных служб инфокоммуникационной системы организации; - обеспечению безопасности и целостности данных информационных систем и технологий, а также условий жизненного цикла информационных систем; - адаптации приложений к изменяющимся условиям функционирования; - администрированию сетевой подсистемы инфокоммуникационной системы организации. Использовать технологии разработки объектов профессиональной деятельности в различных областях.	
Знать:	ПК-1-31 – Знать механизмы аутентификации и идентификации при доступе к информационным ресурсам; ПК-1-32 – Знать основные криптографические алгоритмы; ПК-1-33- Знать основные веб-уязвимости и веб-атаки
Уметь:	ПК-1-У1 – Уметь проводить анализ устойчивости различных криптографических алгоритмов ПК-1-У2 – Уметь проводить анализ устойчивости хешей паролей пользователей
Владеть:	ПК-1-В1 – Владеть навыками реализации различных криптографических алгоритмов ПК-1-В2– Владеть навыками реализации различных хэш-функций и электронно-цифровых подписей ПК-1-В3– Владеть навыками реализации защиты от веб-угроз

4. СТРУКТУРА И СОДЕРЖАНИЕ						
Код занятия	Наименование разделов и тем /вид занятия/	С е м е с тр	Часов	Компетенции	Литература и эл. ресурсы	Примечание
	Раздел 1. Основные понятия и определения. Виды угроз					
1.1	Основные понятия и определения. Виды угроз /Лек/	7	2	УК-1-31 УК-1-32	Л 1.2 Л 1.3 Л 2.2 Э 1	
1.2	Проработка лекционного материала. Самостоятельное изучение литературы. /Ср/	7	2	УК-1-31 УК-1-32 УК-1-У1	Л 1.2 Л 1.3 Л 2.2 Э 1	
	Раздел 2. Социальная инженерия					
2.1	Социальная инженерия /Лек/	7	2	УК-1-31 УК-1-32	Э 1	
2.2.	Использование утилит для сбора информации из открытых источников /Лр/	7	3	ОПК-3-У1 ОПК-3-В1 УК-1-У1	Л3.4	
2.3	Использование Social engineering toolkit в Kali Linux/Лр/	7	3	ОПК-3-У1 ОПК-3-В1 УК-1-У1	Л3.4	
2.4	Проработка лекционного материала. Самостоятельное изучение литературы. Подготовка к практическим занятиям. /Ср/	7	2	УК-1-31 УК-1-32 УК-1-У1	Э 1	
	Раздел 3. Понятия криптографии. Симметричные криптосистемы					
3.1	Понятия криптографии. Симметричные криптосистемы /Лек/	7	2	ПК-1-32	Л 1.1 Л 1.2 Л 1.3	

					Л 2.1 Л 2.2 Э 1	
3.2	Шифрование данных методом замены в симметричных криптосистемах /Пр/	7	2	ПК-1-32 ПК-1-В1	Л 3.2 Э 1	
3.3	Шифрование с использованием метода гаммирования и датчиков псевдослучайных чисел. Одноразовые блокноты /Пр/	7	2	ПК-1-32 ПК-1-В1	Л 3.2 Э 1	
3.4	Использование утилит взлома паролей /Лр/	7	4	ОПК-3-У1 ОПК-3-В1	Л3.4	
3.5	Проработка лекционного материала. Самостоятельное изучение литературы. Подготовка к практическим занятиям. Выполнение домашних заданий. /Ср/	7	3	ПК-1-32 ПК-1-В1 ПК-1-У1	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Л 3.2 Л 3.3 Э 1	
	Раздел 4. Асимметричные криптосистемы. Электронная цифровая подпись и хэш-функции. Криптоанализ					
4.1	Асимметричные криптосистемы /Лек/	7	2	ПК-1-32 ПК-1-31	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Э 1	
4.2	Электронная цифровая подпись и хэш-функции. Криптоанализ /Лек/	7	1	ПК-1-31 ПК-1-32	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Э 1	
4.3.	Шифрование данных в асимметричной криптосистеме RSA/Пр/	7	3	ПК-1-32 ПК-1-В1 ПК-1-У1	Л 3.2 Э 1	
4.4	Алгоритм Диффи-Хелмана для безопасного обмена ключами/Пр/	7	3	ПК-1-32 ПК-1-В1 ПК-1-У1	Л 3.2 Э 1	
4.5	Алгоритм электронной цифровой подписи RSA /Пр/	7	3	ПК-1-32 ПК-1-В1 ПК-1-У1 ПК-1-В2 ПК-1-У2	Л 3.2 Э 1	
4.6	Алгоритм электронной цифровой подписи Эль-Гамала /Пр/	7	4	ПК-1-32 ПК-1-В1 ПК-1-У1 ПК-1-В2 ПК-1-У2	Л 3.2 Э 3	
4.7.	Проработка лекционного материала. Самостоятельное изучение литературы. Подготовка к практическим занятиям. Выполнение домашнего задания /Ср/	7	3	ПК-1-31 ПК-1-32 ПК-1-В1 ПК-1-У1 ПК-1-У2	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2	

					Л 3.2 Э 1	
	Раздел 5. Блокчейн и криптовалюта)					
5.1	Блокчейн и криптовалюта /Лек/	7	2	ПК-1-31 ПК-1-32	Э 1	
5.2	Проработка лекционного материала. Самостоятельное изучение литературы /Ср/	7	3	ПК-1-31 ПК-1-32	Э 1	
	Раздел 6. Идентификация и аутентификация	7				
6.1	Идентификация и аутентификация/Лек/	7	2	ПК-1-31	Л 1.1 Э 1	
6.2	Проработка лекционного материала. Самостоятельное изучение литературы /Ср/	7	3	ПК-1-31	Л 1.1 Э 1	
	Раздел 7. Веб-уязвимости					
7.1	Веб-уязвимости/Лек/	7	2	ПК-1-33	Л 1.1 Э 1	
7.2	SQL инъекции /Лр/	7	3	ПК-1-33 УК-1-В1 ПК-1-В3 ОПК-2-В1 ОПК-2-У1 ОПК-2-31	Л3.4	
7.3	Разновидности XSS атак/Лр/	7	4	ПК-1-33 УК-1-В1 ПК-1-В3 ОПК-2-В1 ОПК-2-У1 ОПК-2-31	Л3.4	
7.4	Проработка лекционного материала. Самостоятельное изучение литературы /Ср/	7	3	ПК-1-33 УК-1-В1 ОПК-2-В1 ОПК-2-У1 ОПК-2-31	Л 1.1 Э 1	
	Раздел 8. Правовое регулирование					
8.1	Правовое регулирование /Лек/	7	2	ОПК-3-31	Л 1.1 Л 1.2 Л 1.3 Э 1	
8.2	Проработка лекционного материала. Самостоятельное изучение литературы /Ср/	7	2	ОПК-3-31	Л 1.1 Л 1.2 Л 1.3 Э 1	
	Часы на контроль /Контроль/	7	36	УК-1-31 УК-1-32 УК-1-У1 УК-1-В1 ОПК-3-31 ОПК-3-У1 ОПК-3-В1	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Л 3.1 Л 3.2	

				ПК-1-31 ПК-1-32 ПК-1-33 ПК-1-У1 ПК-1-У2 ПК-1-В1 ПК-1-В2 ПК-1-В3 ОПК-2-В1 ОПК-2-У1 ОПК-2-31	Л 3.3	
--	--	--	--	--	-------	--

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

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

Раздел 1. Основные понятия и определения. Виды угроз

1. Понятие защиты информации. Комплекс мер безопасности. (УК-1-31)
2. Техногенные, антропогенные и стихийные источники угроз защиты информации (УК-1-32)
3. Внешние и внутренние угрозы. Умышленные и неумышленные угрозы (УК-1-32)
4. Классификация угроз безопасности по способам воздействия на объекты информационной безопасности угрозы (УК-1-32)

Раздел 2. Социальная инженерия

1. Определение социальной инженерии. Схема социальной инженерии (УК-1-31)
2. Претекстинг. Фишинг. Плечевой серфинг (УК-1-32)
3. Смишинг. Вишинг. Телефонное мошенничество (УК-1-32)
4. Дорожное яблоко. Троянские программы. Кви про кво (УК-1-32)
5. «Пляшущие свинки». Сбор информации из открытых источников. Способы повышения защиты от социальной инженерии (УК-1-32)

Раздел 3. Понятия криптографии. Симметричные криптосистемы

1. Основные понятия криптографии (ПК-1-32)
2. Абсолютно устойчивые криптосистемы по Шеннону и Керкгоффса (ПК-1-32)
3. Симметричные криптосистемы. Основные понятия (ПК-1-32)
4. Классификация симметричных криптоалгоритмов (ПК-1-32)
5. Шифр цезаря. Аффинный шифр (ПК-1-32)
6. Одноразовые блокноты. Гаммирование (ПК-1-32)
7. Блочные и поточные шифры. Основные понятия (ПК-1-32)
8. Сеть Фейстеля (ПК-1-32)
9. Алгоритм DES (ПК-1-32)
10. Алгоритм МАГМА (ПК-1-32)
11. Алгоритм Rijndael (ПК-1-32)
12. Алгоритм RC4 (ПК-1-32)

Раздел 4. Асимметричные криптосистемы. Электронная цифровая подпись и хэш-функции. Криптоанализ

1. Асимметричные криптосистемы (ПК-1-32)
2. Односторонние функции (ПК-1-32)
3. Метод Эль-Гамала (ПК-1-32)
4. Метод RSA (ПК-1-32)
5. Метод Диффи-Хелманна (ПК-1-32)
6. Хэш-функции. Свойства. (ПК-1-32, ПК-1-31)
7. ЭЦП. Свойства (ПК-1-32, УК-1-33)
8. «Хорошая» хэш-функция (ПК-1-32, ПК-1-31)
9. Основные понятия криптоанализа (ПК-1-32)
10. Частотный анализ, метод полного перебора и метод встречи по середине (парадокс дней рождений) (ПК-1-32)
11. Задачи факторизации и дискретного логарифмирования. (ПК-1-32)
12. «Радужные таблицы» (ПК-1-32, ПК-1-31)
13. «Соленый» хэш(ПК-1-32, ПК-1-31)

Раздел 5. Блокчейн и криптовалюта

1. Понятие блокчейна (ПК-1-32, ПК-1-31)
2. Пример работы биткоина (ПК-1-32, ПК-1-31)
3. Майнинг в сети биткоин (ПК-1-32, ПК-1-31)
4. Преимущества и недостатки блокчейн технологий. Сфера использования (ПК-1-32, ПК-1-31)

Раздел 6. Идентификация и аутентификация

1. СКУД-системы. (ПК-1-31)
2. Идентификация и аутентификация. (ПК-1-31)
3. Штрих-коды и QR-коды. (ПК-1-31)

**Перечень вопросов к домашнему заданию
(ПК-1-32, ПК-1-31, УК-1-У-1, ,ОПК-2-31)**

1. Что такое симметричный криптоалгоритм?
2. Какие вы знаете симметричные шифры?
3. Что такое открытый и закрытый ключ?
4. Что такое мод N?
5. Опишите, для чего используется расширенный алгоритм Евклида
6. Чем отличается аффинный шифр от шифра Цезаря, что у них общего?
7. Как хранятся пароли в различных операционных системах?
8. Что такое хэш-функция
9. Что такое ЭЦП?
10. Чем отличается хэш-функция от ЭЦП?
11. Современные симметричные шифры
12. Особенность шифра RC4
13. Что такое «парадокс дней рождений»
14. Частотный анализ
15. Недостатки частного анализа
16. Факторизация
17. «Соль» к хэшу
18. Радужные таблицы
19. Проблемы вычислительной сложности в шифровании и криптоанализе\
20. Абсолютно устойчивый шифр

Так же предусмотрена курсовая работа на тему:

«Анализ угроз информационной безопасности и способы их решения» (ПК-1-31, ПК-1-33, УК-1-В1 , ПК-1-В3, ОПК-3-У1, ОПК-3-В1)

Содержание курсовой работы:

В курсовой работе необходимо проанализировать угрозы информационной безопасности и предложить решения по их минимизации

1. Проанализировать внутренние угрозы и предложить пути их устранения
2. Проанализировать внешние угрозы и пути их устранения
3. Нарисовать схему информационной безопасности

Перечень вопросов к защите курсовой работы
(ПК-1-31, ПК-1-33)

4. Чем отличаются внутренние и внешние угрозы
5. Как следует защищаться от внутренних угроз
6. Как защититься от НСД
7. Какие вы знаете современные сетевые экраны
8. Как защититься от различного рода инъекций
9. Как защититься от вирусов
10. Предложите способы резервирования данных
11. Где располагается ваша система
12. Правила хранения и формирования паролей
13. Защита от роботов

Также по дисциплине предусмотрено **5 лабораторных (ОПК-3-У1,ОПК-3-В1, ПК-1-33,УК-1-В1 ,ПК-1-В3, ,ОПК-2-31, ,ОПК-2-У1, ,ОПК-2-В1)**

и 6 практических работ (ПК-1-32,ПК-1-В1,ПК-1-У1,,ПК-1-У2,ПК-1-В2), связанных с реализацией механизмов защиты в современных компьютерных системах

Перечень вопросов к защите лабораторных и практических работ
(ПК-1-33, ПК-1-32)

1. Что такое хэш-функция
2. Что такое симметричный криптоалгоритм?
3. Что такое асимметричный криптоалгоритм?
4. Какие вы знаете симметричные шифры?
5. Что такое открытый и закрытый ключ?
6. Что такое мод N?
7. Опишите, для чего используется расширенный алгоритм Евклида
8. Как хранятся пароли в различных операционных системах?
9. Чем отличается аффинный шифр от шифра Цезаря, что у них общего?
10. Что такое ЭЦП?
11. Чем отличается хэш-функция от ЭЦП?
12. Какие виды хэш-функций вы знаете?

13. Какие вы знаете асимметричные шифры?
14. Можно ли взломать симметричный шифр путем перебора?
15. Можно ли взломать асимметричный шифр путем перебора?
16. Какие основные принципы разработки шифров?
17. Какие вы знаете виды сетевых атак?
18. Что такое фишинг?
19. Что такое DOS-атака?
20. ЭЦП. Свойства
21. Что такое идентификация и аутентификация?
22. Что такое односторонняя функция?
23. Доказано ли существование односторонних функций?
24. Что такое гаммирование?
25. Что такое ПСЧ-датчик?
26. Если докажут существование односторонних функций это хорошо или плохо для криптографии?
27. Если докажут что односторонних функций не существует, это хорошо или плохо для криптографии?
28. Виды аутентификации
29. В чем суть метода Эль-Гамала
30. В чем суть метода RSA
31. В чем суть метода Диффи-Хелмманна
32. Какие рекомендации по размеру ключей в асимметричных криптосистемах?
33. Классификация симметричных криптоалгоритмов
34. Что такое одноразовый блокнот

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

Экзаменационный билет включает в себя фундаментальный теоретический вопрос и прикладной теоретический вопрос из установленного перечня контрольных вопросов, используемых при формировании экзаменационных билетов при оценке знаний обучающихся на экзамене по темам, изложенным в разделах 1-10 данной РПД.
Пример экзаменационного билета:

СТАРООСКОЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ им. А.А.Угарова

(филиал) федерального государственного автономного образовательного учреждения
высшего образования «Национальный исследовательский
технологический университет «МИСИС»

Кафедра автоматизированных и информационных систем управления им. Ю.И.Еременко

090302 Информационные системы и технологии

Профиль – Информационные системы и технологии

Дисциплина «Информационная безопасность»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Технология NAT
2. Принцип работы коммутаторов
3. Дано N узлов, определить маску подсетей для такого количества узлов

Экзаменатор _____ *А.Ю. Соловьев*

Утверждено на заседании кафедры АИСУ

Протоколом №__ от _____ 2023 г.

Зам. зав. кафедрой АИСУ _____ В.А. Петров

Билеты в бумажном виде хранятся на кафедре АИСУ и утверждены ее заведующим (или заместителем зав. кафедрой).

5.4. Методика оценки освоения дисциплины

№ п/п	Вид оценочного средства	Критерий	Оценка
1	Выполнение и защита домашних	Все задачи домашнего задания выполнены без ошибок, либо с не принципиальными ошибками,	«Зачтено»

		заданий	не влияющими на физическую суть результата	
			Задание не выполнено полностью, либо выполнены не все задачи, либо в решении допущены существенные ошибки, неисправленные после собеседования с преподавателем	«Не зачтено»
	2.	Экзамен	Компетенции сформированы. Обучающийся демонстрирует: - глубокие знания содержания изученной дисциплины во взаимосвязи с другими дисциплинами; - способность использовать теоретические знания при выполнении практических заданий; - аргументированные, исчерпывающие ответы на все вопросы по билету, а также дополнительные вопросы экзаменатора; - умение выполнять и обосновывать решение практических заданий высокого уровня сложности; - наличие собственной обоснованной позиции по обсуждаемым вопросам; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.	«Отлично»
			Компетенции сформированы. Обучающийся демонстрирует: - знание основных терминов по содержанию изученной дисциплины; - твердые знания теоретического материала; - умение дать четкие ответы на поставленные вопросы; - умение решать практические задания; - владение основной литературой, рекомендованной программой дисциплины. Допускаются незначительные неточности в ответах на теоретические вопросы и при выполнении практических заданий.	«Хорошо»
			Компетенции сформированы. Обучающийся демонстрирует: - знания теоретического материала по изученной дисциплине; - неполные ответы на основные вопросы, допуская ошибки в ответе; недостаточное понимание сущности излагаемых вопросов; - неточные ответы на дополнительные вопросы; - умение выполнять практические задания без грубых ошибок; - недостаточное владение литературой, рекомендованной программой дисциплины.	«Удовлетворительно»
			Компетенции не сформированы. Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - принципиальные ошибки при ответе на основные вопросы билета, отсутствие знаний и понимания основных терминов и определений; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие навыка или существенные ошибки при выполнении практических заданий; - незнание литературы, рекомендованной программой дисциплины.	«Неудовлетворительно»
	3.	Курсовая работа	Компетенции сформированы. Курсовая работа выполнена в полном объеме; отчёт по работе оформлен в полном соответствии с предъявляемыми требованиями.	«Отлично»

			Компетенции сформированы. Курсовая работа в целом выполнена правильно, расчеты содержат не принципиальные ошибки. Отчёт по работе оформлен в основном в соответствии с предъявляемыми требованиями	«Хорошо»	
			Компетенции сформированы. Курсовая работа в основной части выполнена; отчёт по работе оформлен с некоторыми отступлениями от предъявляемых требований.	«Удовлетворительно»	
			Компетенции не сформированы. Курсовая работа не выполнена, либо отчёт по работе отсутствует или его оформление не соответствует предъявляемым требованиям.	«Неудовлетворительно»	
	4	Устный опрос по материалам лабораторных и практических занятий	Обучающийся уверенно и правильно отвечает на вопросы	«Зачтено»	
			Обучающийся не верно отвечает на вопросы	«Не зачтено»	

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ				
6.1. Рекомендуемая литература				
6.1.1 Основная литература				
Обозначение	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л 1.1	А. В. Зенков.	Информационная безопасность и защита информации : учебное пособие для вузов	ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/530927	Москва : Издательство Юрайт, 2023
Л 1.2	Г. М. Суворова.	Информационная безопасность : учебное пособие для вузов	ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/531084	Москва : Издательство Юрайт, 2023
Л 1.3	Под ред. Поляковой Т. А., Стрельцова А. А	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов	ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/511239	Москва : Издательство Юрайт, 2023
6.1.2 Дополнительная литература				
Обозначение	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л 2.1	Щеглов А. Ю., Щеглов К. А.	Защита информации: основы теории : учебник для вузов	ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/511998	Москва : Издательство Юрайт, 2023
Л 2.2	Внуков А. А.	Защита информации : учебное пособие для вузов	ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/512268	Москва : Издательство Юрайт, 2023
6.1.3. Методические разработки				
Обозначение	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л.3.1	Соловьев А.Ю.	Пособие по выполнению курсовой работы по курсу «Информационная	https://lms.misis.ru/enroll/6MMCH4	

		безопасность»		
Л 3.2	Соловьев А.Ю	Пособие к выполнению практических занятий по курсу «Информационная безопасность»	https://lms.misis.ru/enroll/6MMCH4	
Л 3.3	Соловьев А.Ю	Пособие к выполнению домашних заданий по курсу «Информационная безопасность»	https://lms.misis.ru/enroll/6MMCH4	
Л 3.4	Соловьев А.Ю	Лабораторный практикум по курсу «Информационная безопасность»	https://lms.misis.ru/enroll/6MMCH4	
6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э 1	Защита информации https://openedu.ru/course/hse/DATPRO/			
6.3. Перечень программного обеспечения				
П 1	Microsoft Windows			
П 2	Microsoft office			
П 3	Дистрибутив Kali Linux (свободно распространяемое программное обеспечение)			
П 4	Дистрибутив Ubuntu (свободно распространяемое программное обеспечение)			

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ	
7.1	Аудитория №406 «Лаборатория прикладного программирования» Перечень основного оборудования, учебно-наглядных пособий: • монитор - 9шт.; • персональный компьютер - 9шт.; • проектор; • экран настенный; • усилитель-распределитель; • комплект учебной мебели на 25 посадочных мест.
7.2	Аудитория №404 «Лаборатория объектно-ориентированного программирования» Перечень основного оборудования, учебно-наглядных пособий: • персональный компьютер – 9 шт; • интерактивная доска; • проектор; • комплект учебной мебели на 25 посадочных мест.
7.3	Аудитория №306 «Кабинет для самостоятельной работы» Перечень основного оборудования, учебно-наглядных пособий: • проектор; • доска; • экран настенный; • компьютер – 6 шт.; • комплект учебной мебели на 20 человек. В помещении для самостоятельной работы обучающихся имеется подключение к сети «Интернет» и доступ в электронную информационно-образовательную среду

	организации.
--	--------------

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

Промежуточная аттестация по дисциплине предусмотрена в виде экзамена и курсовой

Обучение проводится в один семестр и организуется в соответствии с настоящей программой. Самостоятельная работа студентов осуществляется и контролируется с помощью:

- индивидуального опроса студентов при защите лабораторных работ и практических занятий,
- сдачи домашних заданий
- защиты курсовой работы

Экзамен проводится при условии выполнения учебного плана дисциплины, и по результатам ответов на экзаменационные билеты