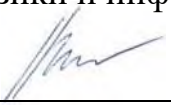
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ ИМЕНИ К.Г. РАЗУМОВСКОГО (ПЕРВЫЙ КАЗАЧИЙ УНИВЕРСИТЕТ)»

УТВЕРЖДАЮ

Заведующий кафедрой Математики физики и информационных технологий



_____Таран В.Н.

«_23_» марта 2022 г.

Рабочая программа дисциплины (модуля)

Б1.О.04.06 ОБЩЕПРОФЕССИОНАЛЬНЫЙ МОДУЛЬ Информационная безопасность

Кафедра:	Математики, физики и информационных технологий
Направление подготовки:	09.03.03 Прикладная информатика
Направленность (профиль):	Проектирование программного обеспечения для бизнеса в пищевой промышленности и отраслях агропромышленного комплекса
Квалификация выпускника:	Бакалавр
Форма обучения:	Очно-заочная
Общая трудоемкость:	216 часов/6 з.е.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00AA7853CEFA35F0837BA866654F3503A6
Владелец: Павлятенко Геннадий Владимирович
Действителен: с 08.12.2025 до 03.03.2027

Ростов-на-Дону, 2022 г.

Рабочая программа дисциплины (модуля)разработана на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03. Прикладная информатика (уровень бакалавриата), утвержденного приказом Министерства образования и науки Российской Федерации от 12.03.2015г. № 207, учебного плана по основной профессиональной образовательной программе высшего образования «Прикладная информатика».

Руководитель основной профессиональной образовательной программы д.ф.-м.н., доцент _____Таран В.Н.
(подпись)

Рабочая программа дисциплины (модуля) обсуждена и утверждена на заседании кафедры «МФиИТ»
Протокол № 6 от «21» марта 2022 года
Заведующий кафедрой д.ф.-м.н., доцент _____Таран В.Н.
(подпись)

д.т.н., доцент, заведующий кафедрой Информационных систем и технологий
ФГБОУ ВО «МГУТУ им.К.Г. Разумовского (ПКУ)» _____С.А. Красников
(подпись)

к.т.н. доцент кафедры Информационных систем и технологий ФГБОУ ВО «МГУТУ им. К.Г. Разумовского (ПКУ)» _____М.В. Сартаков
(подпись)

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ И ОБЪЕМ С РАСПРЕДЕЛЕНИЕМ ПО СЕМЕСТРАМ

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

6. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

9. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цели:

Цель учебной дисциплины заключается в получении обучающимися теоретических
знаний об основах защиты информации, организационных методах защиты информации, математических методах, лежащих в основе защиты информации с последующим применением в профессиональной сфере

1.2. Задачи:

1. изложение системы основных концепций и понятий, используемых в современных технологиях защиты информации;
2. описание основных подходов, принятых в сфере информационной безопасности;
3. ознакомление с основными инструментальными средствами защиты информации;
4. приобретение навыков работы с аппаратными средствами защиты информации;
5. формирование навыков самостоятельной работы, организации
исследовательской работы

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ И ОБЪЕМ С РАСПРЕДЕЛЕНИЕМ ПО СЕМЕСТРАМ

Цикл (раздел) ОП: Б1.О

Дисциплина относится к обязательной части ОПОП и обязательна для освоения.

Связь с предшествующими дисциплинами (модулями), практиками

№ п/п	Наименование	Семестр	Шифр компетенции
1	Технологическая (проектно-технологическая) практика	4	УК-6, ОПК-3, ОПК-4, ОПК-5, ОПК-6, ОПК-7, УК-1, УК-2, УК-3, УК-4, УК-8, ОПК-1, ОПК-8, ОПК-9, УК-5, УК-9, ОПК-2

Распределение часов дисциплины

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		**7 (4.1)**		Итого	
Недель	17 1/6		17 2/6			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	16	16	16	16	32	32
Лабораторные			16	16	16	16
Практические	16	16	16	16	32	32
Итого ауд.	32	32	48	48	80	80
Контактная работа	32	32	48	48	80	80
Сам. работа	40	40	69	69	109	109
Часы на контроль			27	27	27	27
Итого	72	72	144	144	216	216

Вид промежуточной аттестации:

Зачёт 6 семестр

Экзамен 7 семестр

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций и индикаторов их

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;

ОПК-3.1: Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.2: Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.3: Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

Компетенция	Способен	Знает	Умеет	Владеет
ОПК-3	**решать стандартные**	принципы, методы	решать стандартные	навыками подготовки

	задачи профессиональной деятельности на основе информационной и библиографическо й культуры с применением информационно-коммуникационны х технологий и с учетом основных требований информационной безопасности;	и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографическо й культуры с применением информационно-коммуникационны х технологий и с учетом основных требований информационной безопасности	задачи профессиональной деятельности на основе информационной и библиографическо й культуры с применением информационно-коммуникационны х технологий и с учетом основных требований информационной безопасности	обзоров, аннотаций, составления рефератов, научных докладов, публикаций,и библиографии по научно-исследовательско й работе с учетом требований информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименования разделов, тем, их краткое содержание и результаты освоения /вид занятия/	Семестр	Часов	Интеракт.	Прак. подг.	Индикаторы достижения компетенции	Оценочные средства
	Раздел 1.Информационная безопасность						
1.1	**Тема 1 Правовые основы информационной безопасности в Российской Федерации** **Цель: изучить правовые основы информационной безопасности в Российской Федерации** **Краткое содержание: Нормативно-правовые акты регламентирующие деятельность, связанную с защитой информации на территории РФ. Документы, демонстрирующие государственную политику РФ в сфере защиты информации.** **Предполагаемые результаты:** **ЗНАТЬ основные нормативно-правовые акты и документы регламентирующие деятельность, связанную с информационной безопасностью** **УМЕТЬ ориентироваться в основных нормативно-правовых актах и документах регламентирующих деятельность, связанную с информационной безопасностью** **ВЛАДЕТЬ навыками работы с основными нормативно-правовыми актами и документами регламентирующими деятельность, связанную с информационной безопасностью**	6	8	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	Тестирование
1.2	**Тема 2 Физические основы передачи информации. Технические средства защиты информации. История технологий шифрования. Модульная арифметика. Элементы коммутативной алгебры. Элементы элементарной теории чисел** **Цель: изучить физические основы передачи информации, технические средства защиты информации, историю технологий шифрования, модульную арифметику, элементы коммутативной алгебры и элементарной теории чисел** **Краткое содержание: Основные физические принципы используемые для передачи информации с использованием электромагнитных волн, даются основные формулы, для расчёта характеристик каналов связи, размеров приёмопередающих антенн, оценки параметров несущих частот. Меры необходимые для обеспечения доступности и целостности информации передаваемой по средствам электромагнитных волн.**	6	8	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	Тестирование

	Технические средства защиты информации, технические средства перехвата информации, даются классификации технических средств, обсуждаются вопросы, связанные с концептуальным, комплексным подходом к защите информации от утечек по техническим каналам. Меры необходимые для обеспечения сохранности информации представляющей коммерческую или иную ценность. Первые системы шифрования, даётся общий взгляд на развитие отрасли информационной безопасности и шифрования в частности в историческом процессе, перечисляются ключевые фигуры, сыгравшие роль в развитии технологий криптографической защиты информации. Операции с числами по модулю, вводятся понятия сравнимости по модулю, объясняется принцип проведения основных арифметических операций по модулю. Приводится решение типичных задач. Понятие кольца вычетов, перечисляются основные свойства. Понятие поля. Функция Эйлера. Решение типичных задач. Общее представление о таких, важных в криптографии понятиях, как делимость целых чисел, НОД, разложение на простые множители. расширенный алгоритм Евклида, Малая теорема Ферма, КТО. Решение типичных задач. Предполагаемые результаты: ЗНАТЬ основные физические принципы передачи информации, технические средства защиты информации УМЕТЬ обеспечивать доступность и целостность передаваемой информации ВЛАДЕТЬ арифметическими операциями по модулю /Лек/						
1.3	**Тема 3 Алгоритмы симметричного и ассиметричного шифрования. Использование шифрования в системах защиты информации. Особенности программной реализации криптоаналитических алгоритмов и алгоритмов шифрования. Уязвимости интернет страниц. Сетевая безопасность Цель: изучить алгоритмы симметричного и ассиметричного шифрования, принципы сетевой безопасности Краткое содержание: Информация о структуре и правилах построения современных симметричных шифров, строится примитив системы шифрования на базе**	7	16	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	Тестирование

	алгоритма DES. Наиболее распространённые алгоритмы симметричного шифрования, обсуждаются режимы шифрования, их достоинства и недостатки. Структуре и правила построения современных асимметричных шифров, построение системы шифрования на базе алгоритма RSA. Общее представление, о месте технологий шифрования в структуре ИБ, рекомендации по выбору тех или иных решений при построении защищённых систем. Структура алгоритмов ЭЦП. Практическое применение методов атаки на много и одно–алфавитные шифры замены. Структура системы симметричного и ассиметричного шифрования, проблемы использования BSD арифметики, и алгоритмов её реализующих. Современные методы XSS и CSRF атак на интернет ресурсы принципы их работы, возможные методы защиты. Уязвимости телекоммуникационных сетей и методы их защиты. Внедрение/настройка стандартных средств обеспечения информационной безопасности систем SAP (стойкость и время действия паролей, длительность сессий, параметры SSO и др.). Аудит ролей и полномочий SAP Business Suite (R/3, BW, Enterprise Portal, BusinessObjects), проектирование и корректировка ролевых моделей. Анализ угроз информационной безопасности корпоративных информационных систем, формирование рекомендаций, разработка мер противодействия. Предполагаемые результаты: ЗНАТЬ алгоритмы симметричного и ассиметричного шифрования, особенности программной реализации криптоаналитических алгоритмов и алгоритмов шифрования, уязвимости интернет страниц УМЕТЬ использовать шифрование в системах защиты информации ВЛАДЕТЬ основными методами и принципами обеспечения сетевой безопасности /Лек/						
1.4	**Тема 1 Правовые основы информационной безопасности в Российской Федерации Цель: изучить правовые основы информационной безопасности в Российской Федерации Краткое содержание: Нормативно-правовые акты регламентирующие деятельность, связанную с защитой информации на территории РФ.**	6	2	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	тестирование

	Документы, демонстрирующие государственную политику РФ в сфере защиты информации. /Пр/						
1.5	**Тема 1 Правовые основы информационной безопасности в Российской Федерации Цель: изучить правовые основы информационной безопасности в Российской Федерации Краткое содержание: Нормативно-правовые акты регламентирующие деятельность, связанную с защитой информации на территории РФ. Документы, демонстрирующие государственную политику РФ в сфере защиты информации. /Ср/**	6	20	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	Тестирование
1.6	**Тема 2 Физические основы передачи информации. Технические средства защиты информации. История технологий шифрования. Модульная арифметика. Элементы коммутативной алгебры. Элементы элементарной теории чисел Цель: изучить физические основы передачи информации, технические средства защиты информации, историю технологий шифрования, модульную арифметику, элементы коммутативной алгебры и элементарной теории чисел Краткое содержание: Основные физические принципы используемые для передачи информации с использованием электромагнитных волн, даются основные формулы, для расчёта характеристик каналов связи, размеров приёмопередающих антенн, оценки параметров несущих частот. Меры необходимые для обеспечения доступности и целостности информации передаваемой по средствам электромагнитных волн. Технические средства защиты информации, технические средства перехвата информации, даются классификации технических средств, обсуждаются вопросы, связанные с концептуальным, комплексным подходом к защите информации от утечек по техническим каналам. Меры необходимые для обеспечения сохранности информации представляющей коммерческую или иную ценность. Первые системы шифрования, даётся общий взгляд на развитие отрасли информационной безопасности и шифрования в частности в историческом процессе, перечисляются ключевые фигуры, сыгравшие роль в развитии**	6	14	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	тестирование

	технологий криптографической защиты информации. Операции с числами по модулю, вводятся понятия сравнимости по модулю, объясняется принцип проведения основных арифметических операций по модулю. Приводится решение типичных задач. Понятие кольца вычетов, перечисляются основные свойства. Понятие поля. Функция Эйлера. Решение типичных задач. Общее представление о таких, важных в криптографии понятиях, как делимость целых чисел, НОД, разложение на простые множители. расширенный алгоритм Евклида, Малая теорема Ферма, КТО. Решение типичных задач. /Пр/						
1.7	**Тема 2 Физические основы передачи информации. Технические средства защиты информации. История технологий шифрования. Модульная арифметика. Элементы коммутативной алгебры. Элементы элементарной теории чисел Цель: изучить физические основы передачи информации, технические средства защиты информации, историю технологий шифрования, модульную арифметику, элементы коммутативной алгебры и элементарной теории чисел Краткое содержание: Основные физические принципы используемые для передачи информации с использованием электромагнитных волн, даются основные формулы, для расчёта характеристик каналов связи, размеров приёмопередающих антенн, оценки параметров несущих частот. Меры необходимые для обеспечения доступности и целостности информации передаваемой по средствам электромагнитных волн. Технические средства защиты информации, технические средства перехвата информации, даются классификации технических средств, обсуждаются вопросы, связанные с концептуальным, комплексным подходом к защите информации от утечек по техническим каналам. Меры необходимые для обеспечения сохранности информации представляющей коммерческую или иную ценность. Первые системы шифрования, даётся общий взгляд на развитие отрасли информационной безопасности и шифрования в частности в историческом процессе,**	6	20	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	Тестирование

	перечисляются ключевые фигуры, сыгравшие роль в развитии технологий криптографической защиты информации. Операции с числами по модулю, вводятся понятия сравнимости по модулю, объясняется принцип проведения основных арифметических операций по модулю. Приводится решение типичных задач. Понятие кольца вычетов, перечисляются основные свойства. Понятие поля. Функция Эйлера. Решение типичных задач. Общее представление о таких, важных в криптографии понятиях, как делимость целых чисел, НОД, разложение на простые множители. расширенный алгоритм Евклида, Малая теорема Ферма, КТО. Решение типичных задач. /Ср/						
1.8	**Экзамен /Экзамен/**	7	27	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	Вопросы к экзамену
1.9	**Тема 3 Алгоритмы симметричного и ассиметричного шифрования. Использование шифрования в системах защиты информации. Особенности программной реализации криптоаналитических алгоритмов и алгоритмов шифрования. Уязвимости интернет страниц. Сетевая безопасность Цель: изучить алгоритмы симметричного и ассиметричного шифрования, принципы сетевой безопасности Краткое содержание: Информация о структуре и правилах построения современных симметричных шифров, строится примитив системы шифрования на базе алгоритма DES. Наиболее распространённые алгоритмы симметричного шифрования, обсуждаются режимы шифрования, их достоинства и недостатки. Структуре и правила построения современных асимметричных шифров, построение системы шифрования на базе алгоритма RSA. Общее представление, о месте технологий шифрования в структуре ИБ, рекомендации по выбору тех или иных решений при построении защищённых систем. Структура алгоритмов ЭЦП. Практическое применение методов атаки на много и одно–алфавитные шифры замены. Структура системы симметричного и ассиметричного шифрования, проблемы использования BSD арифметики, и алгоритмов её реализующих. Современные методы XSS и CSRF атак на**	7	69	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	Тестирование

	интернет ресурсы принципы их работы, возможные методы защиты. Уязвимости телекоммуникационных сетей и методы их защиты. Внедрение/настройка стандартных средств обеспечения информационной безопасности систем SAP (стойкость и время действия паролей, длительность сессий, параметры SSO и др.). Аудит ролей и полномочий SAP Business Suite (R/3, BW, Enterprise Portal, BusinessObjects), проектирование и корректировка ролевых моделей. Анализ угроз информационной безопасности корпоративных информационных систем, формирование рекомендаций, разработка мер противодействия. /Ср/						
1.10	**Тема 3 Алгоритмы симметричного и ассиметричного шифрования. Использование шифрования в системах защиты информации. Особенности программной реализации криптоаналитических алгоритмов и алгоритмов шифрования. Уязвимости интернет страниц. Сетевая безопасность Цель: изучить алгоритмы симметричного и ассиметричного шифрования, принципы сетевой безопасности Краткое содержание: Информация о структуре и правилах построения современных симметричных шифров, строится примитив системы шифрования на базе алгоритма DES. Наиболее распространённые алгоритмы симметричного шифрования, обсуждаются режимы шифрования, их достоинства и недостатки. Структуре и правила построения современных асимметричных шифров, построение системы шифрования на базе алгоритма RSA. Общее представление, о месте технологий шифрования в структуре ИБ, рекомендации по выбору тех или иных решений при построении защищённых систем. Структура алгоритмов ЭЦП. Практическое применение методов атаки на много и одно–алфавитные шифры замены. Структура системы симметричного и ассиметричного шифрования, проблемы использования BSD арифметики, и алгоритмов её реализующих. Современные методы XSS и CSRF атак на интернет ресурсы принципы их работы, возможные методы защиты. Уязвимости**	7	16	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	Отчет по лабораторным работам

	телекоммуникационных сетей и методы их защиты. Внедрение/настройка стандартных средств обеспечения информационной безопасности систем SAP (стойкость и время действия паролей, длительность сессий, параметры SSO и др.). Аудит ролей и полномочий SAP Business Suite (R/3, BW, Enterprise Portal, BusinessObjects), проектирование и корректировка ролевых моделей. Анализ угроз информационной безопасности корпоративных информационных систем, формирование рекомендаций, разработка мер противодействия. /Лаб/						
1.11	**Зачет /Зачёт/**	6	0	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы к хачету
1.12	**Тема 3 Алгоритмы симметричного и ассиметричного шифрования. Использование шифрования в системах защиты информации. Особенности программной реализации криптоаналитических алгоритмов и алгоритмов шифрования. Уязвимости интернет страниц. Сетевая безопасность Цель: изучить алгоритмы симметричного и ассиметричного шифрования, принципы сетевой безопасности Краткое содержание: Информация о структуре и правилах построения современных симметричных шифров, строится примитив системы шифрования на базе алгоритма DES. Наиболее распространённые алгоритмы симметричного шифрования, обсуждаются режимы шифрования, их достоинства и недостатки. Структуре и правила построения современных асимметричных шифров, построение системы шифрования на базе алгоритма RSA. Общее представление, о месте технологий шифрования в структуре ИБ, рекомендации по выбору тех или иных решений при построении защищённых систем. Структура алгоритмов ЭЦП. Практическое применение методов атаки на много и одно–алфавитные шифры замены. Структура системы симметричного и ассиметричного шифрования, проблемы использования BSD арифметики, и алгоритмов её реализующих. Современные методы XSS и CSRF атак на интернет ресурсы принципы их работы, возможные методы защиты. Уязвимости**	7	16	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	тестирование

	телекоммуникационных сетей и методы их защиты. Внедрение/настройка стандартных средств обеспечения информационной безопасности систем SAP (стойкость и время действия паролей, длительность сессий, параметры SSO и др.). Аудит ролей и полномочий SAP Business Suite (R/3, BW, Enterprise Portal, BusinessObjects), проектирование и корректировка ролевых моделей. Анализ угроз информационной безопасности корпоративных информационных систем, формирование рекомендаций, разработка мер противодействия. /Пр/						

Перечень применяемых активных и интерактивных образовательных технологий:
Информационные технологии

Личностно ориентированная технология, способ организации самостоятельной деятельности учащихся, направленный на решение задачи учебного проекта

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Самостоятельная работа студентов (далее СРС) – это один из видов активного обучения, который наряду с усвоением новых знаний и развитием мыслительной деятельности помогает студентам овладеть методами организации учебной деятельности. В зависимости от формы организации различают два вида самостоятельной работы: организуемую преподавателем и внеаудиторную. Организуемая преподавателем самостоятельная работа предусматривает выдачу студентам индивидуальных заданий по данной учебной дисциплине и самостоятельное выполнение их студентами. Внеаудиторную самостоятельную работу студент организует сам. Рекомендуется использовать следующие формы организуемой самостоятельной работы:
– контрольные работы на занятиях;
– работа с научной литературой;
– проектные задания;
– семестровые задания.
Самостоятельная работа студента предусматривает:
– углубленное изучение лекционного и дополнительного теоретического материала;
- подготовку к семинарским занятиям;
Обучение предполагает проведение аудиторных занятий (лекции и практические/лабораторные занятия) и организацию самостоятельной работы студентов. Выполнение домашнего задания является базовой самостоятельной работой, обеспечивающее подготовку студента к текущим аудиторным занятиям и контрольным мероприятиям. Результаты этой подготовки проявляются в активности студента на занятиях и в качестве выполненных контрольных работ, тестовых заданий, написанных рефератов (докладов) и других форм текущего контроля.
Домашние задания оцениваются по системе «зачтено» или «незачтено». Качество выполнения домашнего задания является фактором, влияющим на итоговую оценку по дисциплине.

6. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕ ИАЛЫ

6.1. Перечень компетенций с указанием этапов формирования индикаторов их достижения в процессе освоения ОПОП

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;

Недостаточный уровень:

Знания принципов информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности не сформированы

Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности не сформировано

Не владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности

Пороговый уровень:

Сформированы базовые знания принципов информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности фрагментарно и носит репродуктивный характер

Низкий уровень владения методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности

Продвинутый уровень:

Знания принципов информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности обширные и системные

Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности применяется в решении типовых заданий

Достаточный уровень владения методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности

Высокий уровень:

Знания принципов информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности твердые, аргументированные и всесторонние

Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности применяется в решении как типовых, так и нестандартных творческих заданий

Высокий уровень владения методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности

6.2. Шкала оценивания в зависимости от уровня сформированности компетенций

Уровень сформированности компетенций

Характеристики индикаторов достижения компетенций	**1. Недостаточный: компетенции не сформированы.**	**2. Пороговый: компетенции сформированы.**	**3. Продвинутый: компетенции сформированы.**	**4. Высокий: компетенции сформированы.**
Знания:	Знания отсутствуют.	Сформированы базовые структуры знаний.	Знания обширные, системные.	Знания твердые, аргументированные, всесторонние.
Умения:	Умения не сформированы.	Умения фрагментарны и носят репродуктивный характер.	Умения носят репродуктивный характер применяются к решению типовых заданий.	Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий.
Навыки:	Навыки не сформированы.	Демонстрируется низкий уровень самостоятельности практического навыка.	Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка.

Описание критериев оценивания

Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - допускаются принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой,	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала; -способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные,	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории;

выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкая степень контактности.	рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания, которые следует выполнить.	без грубых ошибок ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; - наличие собственной обоснованной позиции по обсуждаемым вопросам. Возможны незначительные оговорки и неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.	- логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
0 - 59 баллов	**60 - 69 баллов**	**70 - 89 баллов**	**90 - 100 баллов**
Оценка «незачет», «неудовлетворительно»	**Оценка «зачтено/удовлетворительно», «удовлетворительно»**	**Оценка «зачтено/хорошо», «хорошо»**	**Оценка «зачтено/отлично», «отлично»**

Оценочные средства, обеспечивающие диагностику сформированности компетенций, заявленных в рабочей программе по дисциплине (молулю) для проведения промежуточной аттестации

ОЦЕНИВАНИЕ УРОВНЯ ЗНАНИЙ: Теоретический блок вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и излагать материал.
1. Недостаточный уровень
Не владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности
Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности не сформировано
Знания принципов информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности не сформированы
2. Пороговый уровень
Низкий уровень владения методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности
Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности фрагментарно и носит репродуктивный характер
Сформированы базовые знания принципов информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
3. Продвинутый уровень
Достаточный уровень владения методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности
Знания принципов информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности обширные и системные
Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности применяется в решении типовых заданий
4. Высокий уровень
Высокий уровень владения методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности
Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности применяется в решении как типовых, так и нестандартных творческих заданий

Знания принципов информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности твердые, аргументированные и всесторонние

В случае, если сумма рейтинговых баллов, полученных при прохождении промежуточной аттестации составляет от 0 до 9 баллов, то зачет/ зачет с оценкой/ экзамен НЕ СДАН, независимо от итогового рейтинга по дисциплине.
В случае, если сумма рейтинговых баллов, полученных при прохождении промежуточной аттестации находится в пределах от 10 до 30 баллов, то зачет/ зачет с оценкой/ экзамен СДАН, и результат сдачи определяется в зависимости от итогового рейтинга по дисциплине в соответствии с утвержденной шкалой перевода из 100-балльной шкалы оценивания в 5-балльную.
Для приведения рейтинговой оценки по дисциплине по 100-балльной шкале к аттестационной по 5-балльной шкале в соответствии с Положением о балльно-рейтинговой системе оценки успеваемости студентов федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет технологий и управления имени К.Г. Разумовского (Первый казачий университет) используется следующая шкала:

Аттестационная оценка по дисциплине	Рейтинговая оценка по дисциплине
"ОТЛИЧНО"	90 - 100 баллов
"ХОРОШО"	70 - 89 баллов
"УДОВЛЕТВОРИТЕЛЬНО"	60 - 69 баллов
"НЕУДОВЛЕТВОРИТЕЛЬНО"	менее 60 баллов
"ЗАЧТЕНО"	более 60 баллов
"НЕ ЗАЧТЕНО"	менее 60 баллов

6.3. Оценочные средства текущего контроля (примерные темы докладов, рефератов, эссе)
Тема 1

Под информационной безопасностью понимается…
А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.
Б) программный продукт и базы данных должны быть защищены по нескольким направ-лениям от воздействия
В) нет правильного ответа

Защита информации – это..
А) комплекс мероприятий, направленных на обеспечение информационной безопасности.
Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей
В) небольшая программа для выполнения определенной задачи

От чего зависит информационная безопасность?
А) от компьютеров
Б) от поддерживающей инфраструктуры
В) от информации

Основные составляющие информационной безопасности:
А) целостность
Б) достоверность
В) конфиденциальность

Доступность – это…
А) возможность за приемлемое время получить требуемую информационную услугу.
Б) логическая независимость
В) нет правильного ответа

Перечень практических работ
Законодательство РФ в области информационной безопасности

Тема 2

Целостность – это..
А) целостность информации
Б) непротиворечивость информации
В) защищенность от разрушения

Конфиденциальность – это..
А) защита от несанкционированного доступа к информации
Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

Для чего создаются информационные системы?
А) получения определенных информационных услуг
Б) обработки информации
В) все ответы правильные

Целостность можно подразделить:
А) статическую
Б) динамичную
В) структурную

Где применяются средства контроля динамической целостности?
А) анализе потока финансовых сообщений
Б) обработке данных
В) при выявлении кражи, дублирования отдельных сообщений

Перечень практических работ
Изучение положений о государственном лицензировании деятельности в области защиты информации
Изучение положений о сертификации средств защиты информации по требованиям безопасности информации

Перечень лабораторных работ
Обеспечение информационной безопасности предприятий

Тема 3

Какие трудности возникают в информационных системах при конфиденциальности?
А) сведения о технических каналах утечки информации являются закрытыми
Б) на пути пользовательской криптографии стоят многочисленные технические проблемы
В) все ответы правильные

Угроза – это…
А) потенциальная возможность определенным образом нарушить информационную безопасность
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

Атака – это…
А) попытка реализации угрозы
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.

Источник угрозы – это..
А) потенциальный злоумышленник
Б) злоумышленник
В) нет правильного ответа

Окно опасности – это…
А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

Перечень практических работ
Изучение стандартных средств для реализации приложений, использующих симметричное и ассиметричное шифрование
Средства защиты ОС семейства Windows
Изучение возможностей программных закладок, логических «бомб» и «троянских коней»

Перечень лабораторных работ
Защита автоматизированной системы
Обеспечение информационной безопасности предприятий 2
Разработка политики информационной безопасности

6.4. Оценочные средства промежуточной аттестации.
ИТОГОВОЕ ТЕСТИРОВАНИЕ

Под информационной безопасностью понимается…
А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.

В) нет правильного ответа

Защита информации – это..
А) комплекс мероприятий, направленных на обеспечение информационной безопасности.
Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей
В) небольшая программа для выполнения определенной задачи

От чего зависит информационная безопасность?
А) от компьютеров
Б) от поддерживающей инфраструктуры
В) от информации

Основные составляющие информационной безопасности:
А) целостность
Б) достоверность
В) конфиденциальность

Доступность – это…
А) возможность за приемлемое время получить требуемую информационную услугу.
Б) логическая независимость
В) нет правильного ответа

Целостность – это..
А) целостность информации
Б) непротиворечивость информации
В) защищенность от разрушения

Конфиденциальность – это..
А) защита от несанкционированного доступа к информации
Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
В) описание процедур

Для чего создаются информационные системы?
А) получения определенных информационных услуг
Б) обработки информации
В) все ответы правильные

Целостность можно подразделить:
А) статическую
Б) динамичную
В) структурную

Где применяются средства контроля динамической целостности?
А) анализе потока финансовых сообщений
Б) обработке данных
В) при выявлении кражи, дублирования отдельных сообщений

Какие трудности возникают в информационных системах при конфиденциальности?
А) сведения о технических каналах утечки информации являются закрытыми
Б) на пути пользовательской криптографии стоят многочисленные технические проблемы
В) все ответы правильные

Угроза – это…
А) потенциальная возможность определенным образом нарушить информационную безопасность
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

Атака – это…
А) попытка реализации угрозы
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.

Источник угрозы – это..
А) потенциальный злоумышленник
Б) злоумышленник
В) нет правильного ответа

Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

Какие события должны произойти за время существования окна опасности?
А) должно стать известно о средствах использования пробелов в защите.
Б) должны быть выпущены соответствующие заплаты.
В) заплаты должны быть установлены в защищаемой И.С.

Угрозы можно классифицировать по нескольким критериям:
А) по спектру И.Б.
Б) по способу осуществления
В) по компонентам И.С.

По каким компонентам классифицируется угрозы доступности:
А) отказ пользователей
Б) отказ поддерживающей инфраструктуры
В) ошибка в программе

Основными источниками внутренних отказов являются:
А) отступление от установленных правил эксплуатации
Б) разрушение данных
В) все ответы правильные

Основными источниками внутренних отказов являются:
А) ошибки при конфигурировании системы
Б) отказы программного или аппаратного обеспечения
В) выход системы из штатного режима эксплуатации

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:
А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
Б) обрабатывать большой объем программной информации
В) нет правильного ответа

Какие существуют грани вредоносного П.О.?
А) вредоносная функция
Б) внешнее представление
В) способ распространения

По механизму распространения П.О. различают:
А) вирусы
Б) черви
В) все ответы правильные

Вирус – это…
А) код обладающий способностью к распространению путем внедрения в другие программы
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи

Черви – это…
А) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами

Конфиденциальную информацию можно разделить:
А) предметную
Б) служебную
В) глобальную

Природа происхождения угроз:
А) случайные
Б) преднамеренные
В) природные

Предпосылки появления угроз:
А) объективные
Б) субъективные
В) преднамеренные

А) нарушение права собственности
Б) нарушение содержания
В) внешняя среда

Отказ, ошибки, сбой – это:
А) случайные угрозы
Б) преднамеренные угрозы
В) природные угрозы

Отказ - это…
А) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
В) структура, определяющая последовательность выполнения и взаимосвязи процессов

Ошибка – это…
А) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния
Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
В) негативное воздействие на программу

Сбой – это…
А) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
В) объект-метод

Побочное влияние – это…
А) негативное воздействие на систему в целом или отдельные элементы
Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

СЗИ (система защиты информации) делится:
А) ресурсы автоматизированных систем
Б) организационно-правовое обеспечение
В) человеческий компонент

Что относится к человеческому компоненту СЗИ?
А) системные порты
Б) администрация
В) программное обеспечение

Что относится к ресурсам А.С. СЗИ?
А) лингвистическое обеспечение
Б) техническое обеспечение
В) все ответы правильные

По уровню обеспеченной защиты все системы делят:
А) сильной защиты
Б) особой защиты
В) слабой защиты

По активности реагирования СЗИ системы делят:
А) пассивные
Б) активные
В) полупассивные

Правовое обеспечение безопасности информации – это…
А) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) нет правильного ответа

Правовое обеспечение безопасности информации делится:
А) международно-правовые нормы
Б) национально-правовые нормы
В) все ответы правильные

Что относится к государственной тайне?
А) сведения, защищаемые государством в области военной, экономической … деятельности
Б) документированная информация
В) нет правильного ответа

Вредоносная программа - это…
А) программа, специально разработанная для нарушения нормального функционирования систем
Б) упорядочение абстракций, расположение их по уровням
В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

Основополагающие документы для обеспечения безопасности внутри организации:
А) трудовой договор сотрудников
Б) должностные обязанности руководителей
В) коллективный договор

К организационно - административному обеспечению информации относится:
А) взаимоотношения исполнителей
Б) подбор персонала
В) регламентация производственной деятельности

Что относится к организационным мероприятиям:
А) хранение документов
Б) проведение тестирования средств защиты информации
В) пропускной режим

Какие средства используется на инженерных и технических мероприятиях в защите информации:
А) аппаратные
Б) криптографические
В) физические

Программные средства – это…
А) специальные программы и системы защиты информации в информационных системах различного назначения
Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

Криптографические средства – это…
А) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования
Б) специальные программы и системы защиты информации в информационных системах различного назначения
В) механизм, позволяющий получить новый класс на основе существующего

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ:
1. Государственная политика в сфере обеспечения безопасности. Концепция национальной безопасности РФ.
2. Государственная политика в сфере обеспечения информационной безопасности. Доктрина информационной безопасности РФ.
3. Методы обеспечения информационной безопасности России.
4. Источники угроз информационной безопасности России.
5. Виды угроз информационной безопасности России.
6. Правовые методы обеспечения информационной безопасности России.
7. Права человека и информационная безопасность.
8. Ответственность за посягательство на информацию в сфере экономической деятельности.
9. Нормативно-правовые акты РФ по защите государственной тайны. Основные положения закона «О государственной тайне».
10. Роль ФАПСИ, ФСБ, ФСТЭК в обеспечении информационной безопасности России.
11. Определения ТСПИ и ТКУИ.
12. Способы перехвата информации передаваемой ТСПИ.
13. Достоинства и недостатки акустических закладок, в зависимости от их принадлежности к определённому классу (классификация акустических закладок)
14. Методы выявления акустических закладок, в зависимости от класса
15. Шифр Цезаря, простой биграммной замены, самоключ Вижинера, квадраты Кардано.
16. Определение понятий код, номенклатор, открытый текст, шифры замены и перестановки, много- и одно- алфавитные шифры замены, криптоанализ, криптология.
17. Роль Джованни Порта, Этьена Базери, Блеза Виженера, Кергоффса, Клода Шенона, Уитфилда Диффи и Мартина Хеллмана в становлении крптографии.
18. Что означает формулировка числа a и b сравнимы по модулю N
19. Множество значений оператора mod N(т.е. понимать, что это за множество)
20. Какие свойства определяют группы и кольца

29. Тест Ферма
30. Псевдопростые числа по определённому основанию

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ:
1. Решето Эратосфена
2. Теорема Котельникова-Найквиста
3. Принципы проводной передачи данных
4. Принципы беспроводной передачи данных
5. Симметричный алгоритм шифрования
6. Рассеивание и полнота
7. Режимы шифрования
8. Сеть Фейстеля и SP-блоки
9. Вычислительно необратимые функции
10. Какие существуют атаки на алгоритмы шифрования
11. Запас криптостойкости
12. Понятие раунда шифрования
13. Симметричный алгоритм шифрования
14. Рассеивание и полнота
15. Режимы шифрования
16. Определение длинны излучающей антенны
17. Высокочастотное навязывание и методы защиты от него
18. Сеть Фейстеля и SP-блоки
19. Вычислительно необратимые функции
20. Какие существуют атаки на алгоритмы шифрования
21. Запас криптостойкости
22. Понятие раунда шифрования
23. Понятие открытого и закрытого ключа
24. Что такое ассиметричное шифрование, и в каких областях оно используется
25. Алгоритм RSA
26. Виды и способы защиты от XSS атак
27. Виды и способы защиты от CSRF атак
28. Произведение Монтгомери
29. Каким образом осуществляется настройка стандартных средств обеспечения информационной безопасности систем SAP (стойкость и время действия паролей, длительность сессий, параметры SSO и др.).
30. Каким образом осуществляется настройка типовых расширенных средств обеспечения информационной безопасности систем SAP (SAPCRYPTOLIB, Audit, GRC).
31. Аудит ролей и полномочий SAP (R/3, BW, Enterprise Portal, BusinessObjects), проектирование и корректировка ролевых моделей.
32. ИТ-аудит корпоративных информационных систем в части информационной безопасности.
33. Анализ угроз информационной безопасности корпоративных информационных систем, формирование рекомендаций,

6.5. Примерная тематика курсовых работ (проектов)

Учебным планом не предусмотрено

6.6. Методические указания для обучающихся по освоению дисциплины (модуля)

Освоение обучающимся учебной дисциплины предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций и семинаров. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения учебной дисциплины и достижения поставленных целей необходимо внимательно ознакомиться с настоящей рабочей программой учебной дисциплины. Её может представить преподаватель на вводной лекции или самостоятельно обучающийся использует информацию на официальном Интернет-сайте Университета.

Следует обратить внимание на список основной и дополнительной литературы, которая имеется в электронной библиотечной системе Университет, на предлагаемые преподавателем ресурсы информационно-телекоммуникационной сети Интернет. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа.

Обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса:
- знакомит с новым учебным материалом;
- разъясняет учебные элементы, трудные для понимания;
- систематизирует учебный материал;
- ориентирует в учебном процессе.

С этой целью:
- внимательно прочитайте материал предыдущей лекции;
- ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции;
- внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради;
- запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции;
- постарайтесь уяснить место изучаемой темы в своей подготовке;
- узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию,

которой вы владеете по данному вопросу.

Подготовка к лабораторному и практическому занятию.

При подготовке и работе во время лабораторного или практического занятия типа следует обратить внимание на следующие моменты: процесс предварительной подготовки, работа во время занятия, обработка полученных результатов, исправление полученных замечаний.

Предварительная подготовка к учебному лабораторному или практическому занятию заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач лабораторного или практического занятия, техники безопасности при работе в аудитории.

Работа во время учебного лабораторного или практического занятия включает несколько моментов:

- консультирование студентов преподавателями с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач.
- самостоятельное выполнение заданий согласно обозначенной учебной программой тематики.

Обработка, обобщение полученных результатов проводится обучающимися самостоятельно или под руководством преподавателя (в зависимости от степени сложности поставленных задач). Подготовленная к сдаче на контроль и оценку работа сдается преподавателю. Форма отчетности может быть письменная, устная или две одновременно. Главным результатом в данном случае служит получение положительной оценки по каждому лабораторному или практическому занятию. Это является необходимым условием при проведении рубежного контроля и допуска к зачету/экзамену. При получении неудовлетворительных результатов обучающийся имеет право в дополнительное время пересдать преподавателю работу до проведения промежуточной аттестации.

Подготовка к экзамену/зачёту.

К экзамену/зачёту необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить учебную дисциплину в период зачетно-экзаменационной сессии, как правило, не приносят хорошие и отличные результаты.

При подготовке к экзамену/зачёту обратите внимание на практические задания на основе теоретического материала.

При подготовке к ответу на вопросы экзамена/зачёта по теоретической части учебной дисциплины выделите в вопросе главное, существенное (понятия, признаки, классификации и пр.), приведите примеры, иллюстрирующие теоретические положения.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература	
7.1.1. Основная литература	
Л.1.1	Сычев Ю.Н. Защита информации и информационная безопасность [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2022. - 201 с. – Режим доступа: http://znanium.com/catalog/document?id=366835
Л.1.2	Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]:Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2022. - 416 с. – Режим доступа: http://znanium.com/catalog/document?id=364622
Л.1.3	Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2022. - 223 с. – Режим доступа: http://znanium.com/catalog/document?id=364728
7.2. Лицензионное и свободно распространяемое программное обеспечение в том числе отечественного производства	
7.2.1	Microsoft Windows 7
7.2.2	Kaspersky Endpoint Security
7.2.3	Microsoft Office 2013 Standard
7.3. Перечень профессиональных баз данных, информационных справочных систем и ресурсов сети Интернет	
7.3.1	Электронно-библиотечная система "Лань". Режим доступа: https://e.lanbook.com/
7.3.2	Электронно-библиотечная система "Университетская библиотека онлайн". Режим доступа: https://biblioclub.ru/
7.3.3	Электронно-библиотечная система "Znanium.com". Режим доступа: https://znanium.com/
7.3.4	Сайт национального открытого университета "ИНТУИТ". Режим доступа: https://intuit.ru/
7.3.5	Национальный цифровой ресурс "РУКОНТ". Режим доступа: https://rucont.ru/
7.3.6	ПЛАТФОРМА ОНЛАЙН-ОБРАЗОВАНИЯ «РАЗУМ». Режим доступа: https://razoom.mgutm.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1	Адрес: 123007, г. Москва, пр. 3-й Хорошевский, д.1, к.3: аудитория 10-407 - Компьютерный класс, учебная аудитория для занятий лабораторного и практического типа; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации, а также помещение для самостоятельной работы обучающихся : Рабочие места обучающихся; Рабочее место преподавателя, оборудованное компьютером; Доска меловая, интерактивная доска, учебно-наглядные пособия, проектор 5 компьютеров

9. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ

Организация образовательного процесса для лиц с ограниченными возможностями осуществляется в соответствии с «Методическими рекомендациями по организации образовательного процесса для инвалидов и лиц с ограниченными

возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса» Министерства образования и науки РФ от 08.04.2014г. № АК-44/05вн. В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала. Подбор и разработка учебных материалов производится с учетом индивидуальных особенностей. Предусмотрена возможность обучения по индивидуальному графику, при составлении которого возможны различные варианты проведения занятий: в академической группе и индивидуально, на дому с использованием дистанционных образовательных технологий.

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
канд.экон.наук, доц. О.А. Исабекова_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Информационных систем и цифровых технологий
Протокол от_____2023 г. № _
Зав. кафедрой Исабекова О.А._____

Рабочая программа согласована на заседании выпускающей кафедры
Информационных систем и цифровых технологий
Протокол от_____2023 г. № _
Зав. кафедрой Исабекова О.А. _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
канд.экон.наук, доц. О.А. Исабекова_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Информационных систем и цифровых технологий
Протокол от_____2024 г. № _
Зав. кафедрой Исабекова О.А._____

Рабочая программа согласована на заседании выпускающей кафедры
Информационных систем и цифровых технологий
Протокол от_____2024 г. № _
Зав. кафедрой Исабекова О.А. _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
канд.экон.наук, доц. О.А. Исабекова_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Информационных систем и цифровых технологий
Протокол от_____2025 г. № _
Зав. кафедрой Исабекова О.А._____

Рабочая программа согласована на заседании выпускающей кафедры
Информационных систем и цифровых технологий
Протокол от_____2025 г. № _
Зав. кафедрой Исабекова О.А. _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
канд.экон.наук, доц. О.А. Исабекова_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Информационных систем и цифровых технологий
Протокол от_____2026 г. № _
Зав. кафедрой Исабекова О.А._____

Рабочая программа согласована на заседании выпускающей кафедры
Информационных систем и цифровых технологий
Протокол от_____2026 г. № _
Зав. кафедрой Исабекова О.А. _____