

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное автономное образовательное учреждение  
высшего образования

Приложение 4  
к ОПОП ВО 01.04.04 ПРИКЛАДНАЯ МАТЕМАТИКА,  
профиль "Математические методы в искусственном интеллекте  
и анализе данных"

Рабочая программа дисциплины (модуля)

**Современные технологии защиты информации**

Закреплена за подразделением

Кафедра инфокоммуникационных технологий

Направление подготовки

01.04.04 ПРИКЛАДНАЯ МАТЕМАТИКА

Профиль

Математические методы в искусственном интеллекте и анализе данных

Квалификация

**Магистр**

Форма обучения

**очная**

Общая трудоемкость

**5 ЗЕТ**

Часов по учебному плану

180

Формы контроля в семестрах:

в том числе:

экзамен 1

аудиторные занятия

34

курсовая работа 1

самостоятельная работа

110

часов на контроль

36

**Распределение часов дисциплины по семестрам**

Семестр (<Курс>.<Семестр на курсе>)	1 (1.1)		Итого	
Неделя	18			
Вид занятий	уп	рп	уп	рп
Лекции	9	9	9	9
Практические	25	25	25	25
Итого ауд.	34	34	34	34
Контактная работа	34	34	34	34
Сам. работа	110	110	110	110
Часы на контроль	36	36	36	36
Итого	180	180	180	180

Программу составил(и):

*Старший преподаватель, Бахаров Леонид Ефимович*

Рабочая программа

**Современные технологии защиты информации**

Разработана в соответствии с ОС ВО:

Самостоятельно устанавливаемый образовательный стандарт высшего образования - магистратура Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский технологический университет «МИСИС» по направлению подготовки 01.04.04 ПРИКЛАДНАЯ МАТЕМАТИКА (приказ от 02.04.2021 г. № 119 о.в.)

Составлена на основании учебного плана:

01.04.04 Прикладная математика, 01.04.04-МПИМ-24-1.plx Математические методы в искусственном интеллекте и анализе данных, утвержденного Ученым советом НИТУ МИСИС в составе соответствующей ОПОП ВО 22.06.2023, протокол № 5- 23

Утверждена в составе ОПОП ВО:

01.04.04 Прикладная математика, Математические методы в искусственном интеллекте и анализе данных, утвержденной Ученым советом НИТУ МИСИС 22.06.2023, протокол № 5-23

Рабочая программа одобрена на заседании

**Кафедра инфокоммуникационных технологий**

Протокол от 12.04.2023 г., №9

Руководитель подразделения Кузнецова Ксения Александровна

**1. ЦЕЛИ ОСВОЕНИЯ**

1.1	Целью освоения дисциплины является обучение студентов методам обеспечения защиты информации в современных информационных системах (ИС), функционирующих в условиях внешних и внутренних угроз информационной безопасности. Это даст возможность будущему магистру глубоко понимать функционирование механизмов защиты информации в современных ИС, а также решать вопросы формирования политики безопасности, возникающие в ходе проектирования и эксплуатации перспективных ИС. Студенты будут уметь выбирать необходимые протоколы безопасности и предлагать современные методы защиты от новых угроз информационной безопасности; применять методы защиты цифрового контента от угроз модификации и несанкционированного использования при построении ИС; разрабатывать методики построения программной и аппаратной реализации защиты корпоративной сети с учетом применения облачных технологий; моделировать работу алгоритмов защиты информации на базе математического аппарата динамических дискретных систем; анализировать риски функционирования систем защиты информации.
-----	--

**2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

Блок ОП:		Б1.О
2.1	<b>Требования к предварительной подготовке обучающегося:</b>	
2.2	<b>Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:</b>	
2.2.1	Алгоритмизация и программирование	
2.2.2	Искусственный интеллект в задачах распознавания образов	
2.2.3	Методы анализа и обработки естественного языка	
2.2.4	Методы машинного обучения	
2.2.5	Научно-исследовательская практика	
2.2.6	Производственная практика	
2.2.7	Блокчейн - технологии	
2.2.8	Интеллектуальные автономные и мультиагентные системы	
2.2.9	Искусственный интеллект в компьютерных играх	
2.2.10	Искусственный интеллект в медицине	
2.2.11	Искусственный интеллект в финансовых технологиях	
2.2.12	Машинное обучение и методология DevOps при разработке систем искусственного интеллекта	
2.2.13	Научно-исследовательская работа	
2.2.14	Системный подход и генерация знаний в инновациях	
2.2.15	Современные устройства центров обработки больших данных	
2.2.16	Методы искусственного интеллекта в робототехнических системах	
2.2.17	Подготовка к процедуре защиты и защита выпускной квалификационной работы	
2.2.18	Преддипломная практика	
2.2.19	Философия, методология и современные тренды искусственного интеллекта как науки	

**3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ**

<b>ПК-3: Способен обеспечивать организационное и технологическое обеспечение кодирования на языках программирования в рамках выполнения работ и управлению работами по созданию (модификации) и сопровождению ИС.</b>	
<b>Знать:</b>	
ПК-3-31	Методы защиты программного обеспечения от угроз информационной безопасности, методы защиты авторских прав на цифровой контент
ПК-3-32	Основные методики анализа рисков информационной безопасности на предприятии
ПК-3-33	Типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; виды угроз информационных систем и методы обеспечения информационной безопасности; принципы обеспечения информационной безопасности управления предприятием; принципы защиты информации и обеспечения информационной безопасности, сведения об основных угрозах информационной безопасности и их источниках
<b>ОПК-1: Способен обобщать и критически оценивать опыт и результаты научных исследований в области прикладной математики, на основе знаний фундаментальных наук, в междисциплинарных областях</b>	
<b>Знать:</b>	
ОПК-1-31	Методы моделирования поведения нарушителя информационной безопасности. Принципы построения и

функционирования сетей Петри
ОПК-1-33 Основные квантово-механические принципы, лежащие в основе построения квантовых систем защиты информации
ОПК-1-32 Современные методы криптографической и стеганографической защиты информации
<b>ПК-3: Способен обеспечивать организационное и технологическое обеспечение кодирования на языках программирования в рамках выполнения работ и управлению работами по созданию (модификации) и сопровождению ИС.</b>
<b>Уметь:</b>
ПК-3-У1 Использовать концепцию управления рисками при анализе защищенности инфокоммуникационной структуры предприятия
ПК-3-У2 Анализировать угрозы информационной безопасности и уязвимости систем защиты информации, строить модель информационной безопасности с полным перекрытием угроз
ПК-3-У4 Моделировать поведение нарушителя с помощью сети Петри
ПК-3-У3 Применять методы Парето-оптимизации в системе поддержки принятия решений в области проектирования системы защиты информации на предприятии
<b>ОПК-1: Способен обобщать и критически оценивать опыт и результаты научных исследований в области прикладной математики, на основе знаний фундаментальных наук, в междисциплинарных областях</b>
<b>Уметь:</b>
ОПК-1-У3 Производить встраивание цифровых водяных знаков в мультимедийные и программные файлы
ОПК-1-У2 Производить расчет критической длины линии связи при PNS-атаке на квантовый канал
ОПК-1-У1 Применять простейшие методы шифрования и дешифрования текстовой информации, использовать протоколы разделения и разбиения секрета
<b>ПК-3: Способен обеспечивать организационное и технологическое обеспечение кодирования на языках программирования в рамках выполнения работ и управлению работами по созданию (модификации) и сопровождению ИС.</b>
<b>Владеть:</b>
ПК-3-В1 Методикой анализа рисков информационной безопасности при построении системы защиты информации
<b>ОПК-1: Способен обобщать и критически оценивать опыт и результаты научных исследований в области прикладной математики, на основе знаний фундаментальных наук, в междисциплинарных областях</b>
<b>Владеть:</b>
ОПК-1-В1 Методикой генерации псевдослучайных последовательностей для дальнейшего использования в криптографических алгоритмах

#### 4. СТРУКТУРА И СОДЕРЖАНИЕ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Формируемые индикаторы компетенций	Литература и эл. ресурсы	Примечание	КМ	Выполняемые работы
	<b>Раздел 1. Криптографическая защита информации</b>							
1.1	Проблемы современной криптографии /Лек/	1	2	ОПК-1-32	Л1.4 Л1.5 Л1.7Л2.2Л3.6 Э1			
1.2	Изучение протоколов разбиения секрета. Выполнение раздела 1 практической работы № 1 /Пр/	1	2	ОПК-1-У1	Л1.4 Л1.5 Л1.7Л2.2Л3.6 Э1			
1.3	Изучение протоколов разделения секрета. Выполнение раздела 2 практической работы № 1 /Пр/	1	1	ОПК-1-У1	Л1.4 Л1.5 Л1.7Л2.2Л3.6 Э1			Р1
1.4	Подготовка к защите практической работы № 1 /Ср/	1	4	ОПК-1-32 ОПК-1-У1	Л1.4 Л1.5 Л1.7Л2.2Л3.6 Э1		КМ1	

1.5	Практическая работа № 2. Изучение шифра Плейфера /Пр/	1	2	ОПК-1-У1	Л1.4 Л1.5 Л1.7Л2.2Л3.6 Э1			P2
1.6	Подготовка к защите практической работы № 2 /Ср/	1	4	ОПК-1-32 ОПК -1-У1	Л1.4 Л1.5 Л1.7Л2.2Л3.6 Э1		КМ2	
1.7	Практическая работа № 3. Дешифрование шифра простой перестановки при помощи метода биграмм /Пр/	1	2	ОПК-1-У1	Л1.4 Л1.5 Л1.7Л2.2Л3.6 Э1			P3
1.8	Подготовка к защите практической работы № 3 /Ср/	1	4	ОПК-1-У1 ОПК-1-32	Л1.4 Л1.5 Л1.7Л2.2Л3.6 Э1		КМ3	
1.9	Практическая работа № 4. Изучение регистров сдвига с линейной обратной связью как генераторов псевдослучайных чисел /Пр/	1	2	ОПК-1-В1	Л1.5Л2.1Л3.6 Э1			P4
1.10	Подготовка к защите практической работы № 4 /Ср/	1	4	ОПК-1-32 ОПК -1-В1	Л1.5Л2.1Л3.6 Э1		КМ4	
	<b>Раздел 2. Моделирование систем защиты информации</b>							
2.1	Риск-ориентированный подход в системах защиты информации /Лек/	1	2	ПК-3-32	Л1.6Л2.6Л3.2 Э1			
2.2	Обзор методик анализа рисков в системах защиты информации /Лек/	1	1	ПК-3-32	Л1.6Л2.6Л3.4 Э1			
2.3	Практическая работа № 5. Изучение модели информационной безопасности с полным перекрытием угроз /Пр/	1	2	ПК-3-У2	Л1.6Л2.7Л3.2 Э1			P5
2.4	Подготовка к защите практической работы № 5 /Ср/	1	4	ПК-3-32 ПК-3- У2	Л1.6Л2.7Л3.2 Э1		КМ5	
2.5	Практическая работа № 6. Анализ рисков информационной безопасности /Пр/	1	2	ПК-3-У1	Л1.6Л2.6Л3.2 Э1			P6
2.6	Подготовка к защите практической работы № 6 /Ср/	1	4	ПК-3-32 ПК-3- У1	Л1.6Л2.6Л3.2 Э1		КМ6	
2.7	Выполнение курсовой работы по анализу рисков информационной безопасности на заданном объекте /Ср/	1	62	ПК-3-32 ПК-3- В1 ОПК-1-31	Л1.6Л2.6Л3.3 Э1 Э2		КМ13	P13
2.8	Практическая работа № 7. Изучение системы поддержки принятия решений в области проектирования системы защиты информации на предприятии /Пр/	1	2	ПК-3-У3	Л1.6Л2.3 Л2.4Л3.7 Э1			P7

2.9	Подготовка к защите практической работы № 7 /Ср/	1	4	ПК-3-32 ПК-3-У3	Л1.6Л2.3 Л2.4Л3.7 Э1		КМ7	
2.10	Практическая работа № 8. Разработка сценариев действий нарушителя информационной безопасности с использованием сети Петри /Пр/	1	2	ПК-3-У4	Л1.6Л2.7Л3.2 Э1			Р8
2.11	Подготовка к защите практической работы № 8 /Ср/	1	4	ПК-3-32 ПК-3-У4 ОПК-1-31	Л1.6Л2.7Л3.2 Э1		КМ8	
	<b>Раздел 3. Защита цифрового контента от угроз информационной безопасности</b>							
3.1	Технологии защиты электронного документооборота /Лек/	1	2	ПК-3-31 ПК-3-33 ОПК-1-У3	Л1.1 Л1.3Л3.1 Л3.4 Л3.6 Э1			
3.2	Практическая работа № 9. Защита программного обеспечения методами стеганографии /Пр/	1	2	ОПК-1-У3	Л1.1 Л1.3Л3.1 Л3.4 Л3.6 Э1			Р9
3.3	Подготовка к защите практической работы № 9 /Ср/	1	4	ОПК-1-У3 ОПК-1-32	Л1.1 Л1.3Л3.1 Л3.4 Л3.6 Э1		КМ9	
3.4	Практическая работа № 10. Защита электронных документов с использованием цифровых водяных знаков /Пр/	1	2	ОПК-1-У3	Л1.1 Л1.3Л3.1 Л3.4 Л3.6 Э1			Р10
3.5	Подготовка к защите практической работы № 10 /Ср/	1	4	ОПК-1-У3 ОПК-1-32	Л1.1 Л1.3Л3.1 Л3.4 Л3.6 Э1		КМ10	
3.6	Практическая работа № 11. Стегокомплексы, допускающие использование аудиоконтейнеров /Пр/	1	2	ОПК-1-У3	Л1.1 Л1.3Л3.1 Л3.4 Л3.6 Э1			Р11
3.7	Подготовка к защите практической работы № 11 /Ср/	1	4	ОПК-1-У3 ОПК-1-32	Л1.1 Л1.3Л3.1 Л3.4 Л3.6 Э1		КМ11	
	<b>Раздел 4. Квантовые технологии защиты информации</b>							
4.1	Квантовая криптография и перспективы квантовых технологий защиты информации /Лек/	1	2	ОПК-1-33	Л1.2Л2.5Л3.5 Э1			
4.2	Практическая работа № 12. Расчет критической длины линии связи при PNS-атаке на квантовый канал /Пр/	1	2	ОПК-1-У2	Л1.2Л2.5Л3.5 Э1			Р12
4.3	Подготовка к защите практической работы № 12 /Ср/	1	4	ОПК-1-33 ОПК-1-У2	Л1.2Л2.5Л3.5 Э1		КМ12	

## 5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

<b>5.1. Контрольные мероприятия (контрольная работа, тест, коллоквиум, экзамен и т.п), вопросы для самостоятельной подготовки</b>			
Код КМ	Контрольное мероприятие	Проверяемые индикаторы компетенций	Вопросы для подготовки
КМ1	Защита практической работы № 1.	ОПК-1-32;ОПК-1- У1	<p>Для чего необходимо применение шифрования с открытым ключом в тайных многосторонних вычислениях?</p> <p>Как происходит генерация ключей в алгоритме RSA?</p> <p>Что означает <math>(m, n)</math>–пороговая схема разделения секрета.</p> <p>Назначение интерполяционного полинома Лагранжа.</p> <p>Сущность китайской теоремы об остатках.</p> <p>Чем отличается разбиение секрета от разделения секрета?</p> <p>Чем отличается разбиение секрета от тайных многосторонних вычислений?</p>
КМ2	Защита практической работы № 2.	ОПК-1-32;ОПК-1- У1	<p>К какому классу шифров относится шифр Плейфера? Укажите особенности подобных шифров.</p> <p>Опишите процедуры шифрования и расшифрования по методу Плейфера.</p> <p>Оцените криптостойкость изученного метода шифрования и возможности использования подобных методов в современных криптосистемах.</p> <p>Зашифруйте свою фамилию шифром Плейфера вручную. Сравните результаты ручного шифрования и полученные с помощью программы Playfair.exe.</p>
КМ3	Защита практической работы № 3.	ОПК-1-32;ОПК-1- У1	<p>В чем заключается описанный в работе метод вскрытия криптограмм?</p> <p>В чем заключается метод шифрования (расшифрования) с использованием перестановок? Какие перестановочные методы шифрования вы знаете?</p> <p>Приведите примеры использования алгоритма перестановки в современных симметричных криптосистемах.</p> <p>Какие требования к исходным текстам и длинам ключей шифрования обеспечат максимальный эффект для использования изученного метода дешифрования?</p>
КМ4	Защита практической работы № 4.	ОПК-1-В1;ОПК-1- 32	<p>Что такое М-последовательность? Каковы ее свойства? Какая отводная последовательность позволяет ее получить? Опишите процесс работы четырехбитового РгСсЛОС: откуда берется выходной бит и как формируется псевдослучайная последовательность, как происходит сдвиг регистра, как меняется его состояние, как образуется бит функции обратной связи (приведите таблицу истинности для операции XOR от 1, 2, 3, 4 переменных)</p> <p>Что определяет свойство периодичности РгСсЛОС? От чего зависит период РгСсЛОС? Какие многочлены являются неприводимыми по модулю 2? Где и для чего их можно применять на практике?</p> <p>Что входит в понятие «Линейная сложность бинарной последовательности»? Как ее можно использовать для оценки псевдослучайной бинарной последовательности? Что определяет свойство периодичности РгСсЛОС? От чего зависит период РгСсЛОС?</p> <p>Что такое отводная последовательность? Для чего она нужна в РгСсЛОС и на какие его параметры влияет? Что такое инициальное состояние РгСсЛОС? Какие есть ограничения на значение инициального состояния? Почему? Что такое ГСПЧ? На чем они могут быть основаны? Какие у них преимущества и недостатки?</p>

КМ5	Защита практической работы № 5.	ПК-3-31;ПК-3-У2	<p>Что такое угроза информационной безопасности? Приведите примеры.</p> <p>Каким образом могут быть классифицированы угрозы информационной безопасности?</p> <p>Что такое уязвимость и чем она отличается от угрозы?</p> <p>Каким образом может быть проведена классификация уязвимостей?</p> <p>Какие модели защиты информации Вы знаете?</p> <p>Какие предположения лежат в основе модели с полным перекрытием угроз?</p> <p>Назовите преимущества и недостатки модели с полным перекрытием угроз.</p>
КМ6	Защита практической работы № 6.	ПК-3-32;ПК-3-У1	<p>Какая информация должна быть собрана на объекте оценки для проведения анализа информационных рисков?</p> <p>В каких единицах измеряется риск информационной безопасности?</p> <p>Выберите оптимальную стратегию управления рисками в следующем случае: веб-сервер компании находится внутри корпоративной сети и его программное обеспечение, возможно, содержит уязвимости.</p> <p>Какую информацию необходимо получить на объекте оценки для определения ущерба по угрозе «нарушение целостности информации»?</p> <p>Какую информацию необходимо получить на объекте оценки для определения ущерба по угрозе «нарушение конфиденциальности информации»?</p> <p>В случае анализа рисков информационной системы на базовом уровне какими стандартами в области защиты информации необходимо руководствоваться?</p> <p>В случае полного анализа рисков информационных систем какие подходы обычно используются на практике?</p> <p>Какие этапы должен включать аудит информационной безопасности?</p> <p>Как осуществляется анализ информационных рисков, угрозы и уязвимости системы по двум факторам?</p> <p>Как осуществляется анализ информационных рисков, угрозы и уязвимости системы по двум факторам?</p>
КМ7	Защита практической работы № 7.	ПК-3-У3;ПК-3-32	<p>Какие требования предъявляются к набору критериев для оценки альтернативных решений?</p> <p>Как оценивается важность критериев?</p> <p>Приведите классификацию задач принятия решений в области проектирования систем защиты информации.</p> <p>Назовите основные этапы принятия управленческих решений в области построения защищенных систем обработки информации.</p> <p>Приведите пример генерирования множества альтернатив с применением экспертных методов при разработке системы защиты информации.</p> <p>Приведите пример использования метода строчных сумм для составления матрицы альтернативных проектов системы защиты информации.</p> <p>Сформулируйте принцип Парето. В чем достоинства и недостатки его практического применения для принятия управленческих решений в области построения защищенных систем обработки информации?</p> <p>Что понимается под парето-оптимальным множеством?</p> <p>Какие дополнительные возможности предоставляет метод достижимых целей для принятия управленческих решений в области построения защищенных систем обработки информации?</p> <p>Опишите последовательность шагов при использовании парето-оптимизации в выборе альтернативных проектов системы защиты информации.</p>



КМ8	Защита практической работы № 8.	ПК-3-У4;ПК-3-32	<p>В чем отличие сетей Петри от других способов моделирования в системах защиты информации?</p> <p>Каким образом можно интерпретировать позиции и переходы при разработке сценариев действия нарушителя на объекте информатизации с использованием сети Петри? Приведите конкретные примеры.</p> <p>В чем заключается ограниченность использования сетей Петри для моделирования процессов, происходящих в информационных системах?</p> <p>Каким образом можно интерпретировать использование маркеров в сети Петри при моделировании действий нарушителя? Приведите конкретные примеры.</p> <p>Какие выводы можно сделать о достижимости конечной цели атак при запуске разработанной сети Петри?</p>
КМ9	Защита практической работы № 9.	ПК-3-31;ОПК-1-У3	<p>Перечислите способы защиты программных продуктов. Укажите их достоинства и недостатки.</p> <p>Какие методы включает юридическая защита программных продуктов? Охарактеризуйте основные из них.</p> <p>Перечислите основные международные и отечественные источники защиты прав авторов программ.</p> <p>В чем заключается процедура лицензирования программ? Какими нормативными документами регулируется процесс лицензирования программ?</p> <p>Перечислите технические методы защиты программных продуктов. Кратко охарактеризуйте каждый из них.</p> <p>Какие методы стеганографии могут использоваться для защиты программных продуктов?</p> <p>Сравните методы стеганографической защиты и технической защиты ПО.</p> <p>Какие особенности структуры PE-файлов дают возможность эффективного внедрения цифровых водяных знаков?</p> <p>Опишите суть метода внедрения кода в PE-файлы за счет размещения кода в свободном месте программы (интеграция).</p> <p>Какой из методов внедрения кода в PE-файлы используется в программе Filigrana? Опишите суть этого метода, его достоинства и недостатки.</p> <p>Какие способы обнаружения, извлечения и модификации ЦВЗ вы можете предложить для изученного метода защиты ПО?</p>

КМ10	Защита практической работы № 10.	ОПК-1-У3;ОПК-1- 32	<p>Перечислите способы защиты цифровых графических изображений от модификации и несанкционированного использования. Укажите их достоинства и недостатки.</p> <p>В чем особенность робастных, хрупких и полухрупких цифровых водяных знаков? Каковы ограничения в их использования для защиты электронных документов?</p> <p>Перечислите основные международные и отечественные источники защиты прав авторов цифрового графического контента.</p> <p>Алгоритм Хсу и Ву – особенности реализации, достоинства и недостатки.</p> <p>Алгоритм Фридрих – особенности реализации, достоинства и недостатки.</p> <p>Какие методы стеганографии могут использоваться для защиты графических файлов?</p> <p>Сравните методы стеганографической защиты и криптографической защиты.</p> <p>Алгоритм В. А. Митекина – особенности реализации, достоинства и недостатки.</p> <p>В чем заключается усовершенствование алгоритма В.А. Митекина в программных продуктах, использованных в лабораторной работе?</p> <p>Оцените эффективность исследованного алгоритма для встраивания ЦВЗ ?</p> <p>Подсчитайте максимальных объем встраиваемого ЦВЗ в бинарное изображение размером 1024×128 пикселей: а) в блоки 3×3 пикселя, б) в блоки 7×7 пикселей.</p> <p>Подсчитайте максимальных объем встраиваемого ЦВЗ в полутоновое изображение (256 градаций серого) размером 512×256 пикселей:</p> <p>а) в блоки 3×3 пикселя, б) в блоки 7×7 пикселей.</p>
КМ11	Защита практической работы № 11.	ОПК-1-У3;ПК-3-33	<p>Сформулируйте основные отличия стеганографических и криптографических методов защиты информационных ресурсов. В чем достоинства и недостатки каждого из методов?</p> <p>Перечислите шесть основных режимов работы программы Invisible Secrets-4.</p> <p>В каких случаях вы можете порекомендовать использование каждого из режимов?</p> <p>Оцените эффективность работы программы Invisible Secrets-4 с графическими и аудио файлами различных типов. Для этого в режиме “стеганография”стройте данные в контейнеры различных форматов, сравните пустые и заполненные контейнеры, сделайте выводы.</p> <p>При встраивании данных в режиме “стеганография” используйте различные алгоритмы для шифрования встраиваемых данных. Сравните пустые и заполненные контейнеры, как изменяется размер заполненных контейнеров в зависимости от метода шифрования? Почему вы получили такие результаты, обоснуйте.</p>
КМ12	Защита практической работы № 12.	ОПК-1-33;ОПК-1- У2	<p>Какие физические принципы лежат в основе квантовой криптографии?</p> <p>Поясните назначение и принцип работы алгоритма BB84.</p> <p>Опишите алгоритм Беннета. В чем заключаются его особенности?</p> <p>Какие уязвимости квантовых криптосистем Вам известны?</p> <p>Приведите примеры.</p> <p>Что такое квантовая запутанность и в каких приложениях квантовых технологий защиты информации она используется?</p> <p>Опишите протокол квантового распределения ключей с использованием ЭПР.</p> <p>Каким образом может быть осуществлена атака на протокол BB84?</p> <p>Каким образом может быть осуществлена атака на протокол B92?</p> <p>Что такое PNS-атака и каким образом она осуществляется?</p> <p>Что такое критическая длина линии связи и каким образом она вычисляется в случае PNS-атаки?</p>

КМ13	Защита курсовой работы	ПК-3-32;ПК-3-33;ПК-3-31;ПК-3-У1;ПК-3-У2;ПК-3-У4	<p>Что такое управление рисками информационной безопасности? Какие современные стандарты в области информационной безопасности, использующие концепцию управления рисками Вам известны?</p> <p>Перечислите основные этапы построения и использования системы мониторинга информационной безопасности.</p> <p>Назовите основные этапы методики построения систем защиты информации Lifecycle Security.</p> <p>Назовите основные этапы методики построения систем защиты информации Microsoft. Методика построения систем защиты информации CRAMM.</p> <p>Назовите основные этапы методики построения систем защиты информации FRAP.</p> <p>Назовите основные этапы методики построения систем защиты информации OCTAVE.</p> <p>Назовите основные этапы методики построения систем защиты информации RiskWatch.</p> <p>Сформулируйте принцип Парето. Назовите его достоинства и недостатки при принятии управленческих решений в области построения защищенных систем обработки информации.</p> <p>Каким образом Сети Петри можно использовать для моделирования поведения нарушителя в системе защиты информации?</p> <p>Что такое метки в сетях Петри? Каким образом они используются при моделировании системы защиты информации?</p> <p>Что такое позиции в сетях Петри? Каким образом они используются при моделировании системы защиты информации?</p> <p>Что такое разрешенные и запрещенные переходы в сетях Петри? Каким образом они используются при моделировании системы защиты информации?</p>
------	------------------------	---	---

**5.2. Перечень работ, выполняемых по дисциплине (Курсовая работа, Курсовой проект, РГР, Реферат, ЛР, ПР и т.п.)**

Код работы	Название работы	Проверяемые индикаторы компетенций	Содержание работы
P1	Практическая работа №1. Изучение протоколов разбиения и разделения секрета	ОПК-1-32;ОПК-1- У1	Изучение на практических примерах протокола тайных многосторонних вычислений на основе алгоритма RSA, схемы разбиения секрета с помощью гаммирования, схем разделения секрета с помощью интерполяционных полиномов Лагранжа и китайской теоремы об остатках.
P2	Практическая работа № 2. Симметричные криптоалгоритмы. Шифр Плейфера.	ОПК-1-32;ОПК-1- У1	Изучение принципов построения шифров замены на примере шифра Плейфера.
P3	Практическая работа № 3. Дешифрование шифра простой перестановки при помощи метода биграмм.	ОПК-1-32;ОПК-1- У1	Изучение шифров перестановки и простейших методов их криптоанализа
P4	Практическая работа № 4. Изучение регистров сдвига с линейной обратной связью как генераторов псевдослучайных чисел	ОПК-1-В1;ПК-3-33	Изучение принципа работы генератора псевдослучайных последовательностей, основанного на регистре сдвига с линейной обратной связью.

P5	Практическая работа № 5. Изучение модели информационной безопасности с полным перекрытием угроз	ПК-3-32;ПК-3-У1;ПК-3-У2	Изучение принципов построения политик безопасности и моделей информационной безопасности. Составление модели с полным перекрытием угроз на примере конкретного предприятия.
P6	Практическая работа №6. Анализ рисков информационной безопасности	ПК-3-32;ПК-3-У2;ПК-3-В1	Анализ рисков информационной безопасности предприятия по методике СОВИТ.
P7	Практическая работа № 7. Изучение системы поддержки принятия решений в области проектирования системы защиты информации на предприятии	ПК-3-32;ПК-3-У3	Изучение принципов Парето-оптимизации и системы поддержки принятия решений в области проектирования системы защиты информации на предприятии, построенной на основании метода достижимых целей.
P8	Практическая работа № 8. Разработка сценариев действий нарушителя информационной безопасности с использованием сети Петри.	ОПК-1-31;ПК-3-У1;ПК-3-У4	Изучение принципов построения сетей Петри и разработка сценариев действий нарушителя информационной безопасности с их использованием.
P9	Практическая работа № 9. Защита программного обеспечения методами стеганографии	ПК-3-31;ОПК-1-32;ОПК-1-У3	Изучение способов защиты программного обеспечения. Применение стеганографических методов.
P10	Практическая работа № 10. Защита электронных документов с использованием цифровых водяных знаков	ПК-3-31;ОПК-1-32;ОПК-1-У3	Изучение способов защиты электронных документов с использованием цифровых водяных знаков.
P11	Практическая работа № 11. Стегокомплексы, допускающие использование аудиоконтейнеров	ПК-3-31;ОПК-1-У3	Изучение программного комплекса INVISIBLE SECRET и принципов стеганографического встраивания информации в аудиоконтейнеры.
P12	Практическая работа № 12. Расчет критической длины линии связи при PNS-атаке на квантовый канал	ОПК-1-33;ОПК-1-У2	Изучение атак на канал квантовой связи и расчет критической длины линии связи при PNS-атаке на квантовый канал.
P13	Курсовая работа. Анализ рисков информационной безопасности.	ПК-3-32;ПК-3-31;ПК-3-33;ПК-3-У1;ПК-3-У2;ПК-3-У4;ПК-3-В1;ОПК-1-31;ОПК-1-32	Анализ рисков информационной безопасности по заданной методике и выработка рекомендации по построению политики информационной безопасности предприятия.

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

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

Вопросы к экзамену:

ОПК-1-31 Методы моделирования поведения нарушителя информационной безопасности. Принципы построения и функционирования сетей Петри:

Каким образом Сети Петри можно использовать для моделирования поведения нарушителя в системе защиты информации?

Что такое метки в сетях Петри? Каким образом они используются при моделировании системы защиты информации?

Что такое позиции в сетях Петри? Каким образом они используются при моделировании системы защиты информации?

Что такое разрешенные и запрещенные переходы в сетях Петри? Каким образом они используются при моделировании системы защиты информации?

ОПК-1-32 Современные методы криптографической и стеганографической защиты информации:

Назовите основные проблемы и тенденции развития современной криптографии.

Перечислите и поясните актуальные направления современной криптографии.

Что такое эллиптическая криптография? Поясните сущность метода, основные достоинства и недостатки.

Что такое гомоморфное шифрование? Поясните постановку задачи. Чем отличаются полностью гомоморфные и частично гомоморфные криптосистемы?

Где применяется гомоморфное шифрование?

Что такое низкоресурсная криптография? Каково ее практическое применение? Перечислите требования к средствам низкоресурсной криптографии.

В чем заключается протокол тайных многосторонних вычислений? каково его назначение? Приведите пример реализации. Каким образом работают протоколы разбиения секрета? Каково их назначение? приведите пример реализации с помощью гаммирования.

Поясните протокол разделения секрета по схеме Шамира. Каково его назначение? Приведите пример реализации.

Поясните протокол разделения секрета схеме Асмута-Блума и его назначение. Приведите пример реализации.

Как работает биграммный шифра Плейфера? Поясните процедуры шифрования и расшифровывания. Оцените криптостойкость.

Каким образом осуществляется дешифрование шифра простой перестановки методом биграмм? Приведите примеры использования алгоритма перестановки в современных симметричных криптосистемах.

Как работает генератор псевдослучайных последовательностей, основанный на регистре сдвига с линейной обратной связью?

Что такое линейная сложность бинарной последовательности?

Что такое М-последовательность и каковы ее свойства?

ОПК-1-33 Основные квантово-механические принципы, лежащие в основе построения квантовых систем защиты информации:

В чем заключается проблема распределения ключей в системах защиты информации?

Назовите квантово-механические принципы и поясните их использование в информационной безопасности.

Что такое квантовая криптосистема и каково ее назначение?

Поясните принцип действия протокола квантовой криптографии BB84.

Поясните принцип действия протокола квантовой криптографии B92.

Чем отличаются друг от друга квантовые криптосистемы с поляризационным и фазовым кодированием? Приведите примеры.

Назовите наиболее распространенные уязвимости каналов квантового распределения ключей.

Поясните принцип работы систем квантового распределения ключей. Приведите примеры реализации.

Назовите основные виды протоколов квантового распределения ключей. Охарактеризуйте их преимущества и недостатки.

Каковы перспективы развития квантовых технологий защиты информации?

ПК-3-31 Методы защиты программного обеспечения от угроз информационной безопасности, методы защиты авторских прав на цифровой контент:

Назовите цели защиты программного обеспечения.

Каким образом осуществляется юридическая и техническая защита программного обеспечения?

Поясните технику внедрения кода в исполняемые файлы. Приведите классификацию механизмов внедрения.

Какие алгоритмы встраивания цифрового водяного знака в исполняемые файлы Вам известны? Назовите их достоинства и недостатки.

Каким образом осуществляется защита электронных документов с использованием цифровых водяных знаков?

Поясните принцип работы алгоритмов встраивания цифровых водяных знаков в полутоновые и бинарные изображения.

Что такое стеганография и чем она отличается от криптографии?

Что такое робастность изображения и от чего она зависит?

ПК-3-33 Основные угрозы информационной безопасности на предприятии:

Что такое технические способы организации утечки информации? Приведите их классификацию.

Что представляет собой визуально-оптический канал утечки информации? Назовите основные способы противодействия ему.

Что представляют собой акустический и виброакустический канал утечки информации? Назовите основные способы противодействия им.

Что представляет собой электромагнитный канал утечки информации? Назовите основные способы противодействия ему.

Что представляет собой материальный канал утечки информации? Назовите основные способы противодействия ему.

На каких принципах строится система защиты конфиденциальной информации от утечек?

Назовите основные технологии защиты от утечек данных. Приведите их общую характеристику и классификацию.

Опишите DLP-системы, их основные задачи. Каковы требования к DLP-системам? Что такое контекстный контроль и контентная фильтрация в DLP-системе?

Опишите IPS-системы, их основные и дополнительные задачи, технологии детектирования конфиденциальной информации в IPS-системах.

Опишите IRM-системы, их основные задачи и механизмы реализации. В чем заключаются особенности IRM-систем, их достоинства и недостатки?

Что такое IDL-системы? Каковы их основные возможности и механизм реализации? поясните использование IDL-систем для расследования киберпреступлений.

Что такое атрибутный контроль доступа? Каковы его базовые механизмы реализации?

В чем состоит модель с полным перекрытием угроз? Назовите ее достоинства и недостатки.

ПК-3-32 Основные методики анализа рисков информационной безопасности на предприятии:

Что такое управление рисками информационной безопасности?

Какие современные стандарты в области информационной безопасности, использующие концепцию управления рисками Вам известны?

Перечислите основные этапы построения и использования системы мониторинга информационной безопасности.

Назовите основные этапы методики построения систем защиты информации Lifecycle Security.

Назовите основные этапы методики построения систем защиты информации Microsoft. Методика построения систем защиты информации CRAMM.

Назовите основные этапы методики построения систем защиты информации FRAP.

Назовите основные этапы методики построения систем защиты информации OCTAVE.

Назовите основные этапы методики построения систем защиты информации RiskWatch.

Сформулируйте принцип Парето. Назовите его достоинства и недостатки при принятии управленческих решений в области построения защищенных систем обработки информации.

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

Экзаменационная оценка:

Оценка "отлично" выставляется студенту, полностью ответившему на два теоретических вопроса экзаменационного билета, обнаружившему всестороннее, систематическое и глубокое знание учебного материала, предусмотренного программой; усвоившему основную и знакомому с дополнительной литературой по программе; умеющему творчески и осознанно выполнять задания, предусмотренные программой; усвоившему взаимосвязь основных понятий и умеющему применять их к анализу и решению практических задач; безупречно выполнившему в процессе изучения дисциплины все задания, предусмотренные формами текущего контроля;

Оценки "хорошо" заслуживает студент, ответивший полностью на один вопрос экзаменационного билета и ответивший частично на другой вопрос, при этом обнаруживший полное знание учебного материала, предусмотренного программой; успешно выполнивший все задания, предусмотренные формами текущего контроля;

Оценка "удовлетворительно" выставляется студенту, ответившему полностью только на один вопрос экзаменационного билета или допустившему погрешности в ответе на вопросы экзаменационного билета и обладающему необходимыми знаниями для их устранения под руководством преподавателя;

Оценка "неудовлетворительно" выставляется студенту, не ответившему на два вопроса экзаменационного билета, обнаружившему пробелы в знании основного материала, предусмотренного программой, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий; не выполнившему отдельные задания, предусмотренные формами текущего контроля.

Оценка за курсовую работу:

Оценка «отлично» ставится, если:

- курсовая работа выполнена в полном объеме и соответствует заданию;
- пояснительная записка составлена аккуратно, последовательно с учетом требований стандартов по составлению текстовых документов;
- практическая часть курсовой работы выполнена в полном объеме;
- выполнение курсовой работы проходило в полном соответствии со сроками курсового проектирования;
- защита курсовой работы проведена грамотно с демонстрацией всех возможностей рассмотренной методики анализа рисков.

Оценка «хорошо» допускает:

- некоторые отступления от графика выполнения курсового проектирования;
- существование незначительных погрешностей в оформлении пояснительной записки и реализации методики анализа рисков (практической части курсовой работы).
- недостаточно полными рекомендациями по формированию политики безопасности организации.

Оценка «удовлетворительно» допускает:

- существование ошибок, неточностей и непоследовательности при составлении пояснительной записки;
- значительные отступления от требований ЕСКД при выполнении пояснительной записки;
- отсутствие подробного описания рассматриваемых рисков и уязвимостей;
- отсутствие самостоятельности и творческого подхода при формулировке рекомендации по формированию политики безопасности;
- значительное отступление от сроков выполнения курсовой работы;
- недостаточно грамотную защиту и неполную демонстрацию возможностей рассматриваемой методики анализа рисков.

Оценка «неудовлетворительно» допускает:

- несоответствие курсовой работы заданию;
- отсутствие учета требований стандартов по оформлению текстовых документов при составлении пояснительной записки;
- полное отсутствие описания рассматриваемых рисков и уязвимостей;
- существование ошибок и непоследовательности в реализации методики анализа рисков;
- значительное отступление от сроков выполнения курсовой работы;
- неспособность грамотно защитить курсовую работу.

## 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

### 6.1. Рекомендуемая литература

#### 6.1.1. Основная литература

	Авторы, составители	Заглавие	Библиотека	Издательство, год
--	---------------------	----------	------------	-------------------

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л1.1	Фабричнов А. Г., Дёмушкин А. С., Кондрашова Т. В., Кунаев Н. Н.	Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник	Электронная библиотека	Москва: Логос, 2011
Л1.2	Ильичев Е. В., Гринберг Я. С.	Квантовая информатика и квантовые биты на основе сверхпроводниковых джозефсоновских структур: учебник	Электронная библиотека	Новосибирск: Новосибирский государственный технический университет, 2013
Л1.3	Нестеров С. А.	Основы информационной безопасности: учебное пособие	Электронная библиотека	Санкт-Петербург: Издательство Политехнического университета, 2014
Л1.4	Ищукова Е. А., Лобова Е. А.	Криптографические протоколы и стандарты: учебное пособие	Электронная библиотека	Таганрог: Южный федеральный университет, 2016
Л1.5	Кирпичников А. П., Хайбуллина З. М.	Криптографические методы защиты компьютерной информации: учебное пособие	Электронная библиотека	Казань: Казанский национальный исследовательский технологический университет (КНИТУ), 2016
Л1.6	Мельников В. П., Клейменов С. А., Петраков А. М., Клейменов С. А.	Информационная безопасность и защита информации: учеб. пособие для студ. вузов, обуч. по спец. 230201 "Информационные системы и технологии"	Библиотека МИСиС	М.: ACADEMIA, 2008
Л1.7	Костин В. Н.	Методы и средства защиты компьютерной информации. Криптографические методы защиты информации (N 3086): учеб. пособие	Электронная библиотека	М.: [МИСиС], 2018
<b>6.1.2. Дополнительная литература</b>				
	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л2.1	Башлы П. Н., Баранова Е. К., Бабаши А. В.	Информационная безопасность: учебно- практическое пособие: учебное пособие	Электронная библиотека	Москва: Евразийский открытый институт, 2011
Л2.2	Лапонина О. Р.	Криптографические основы безопасности: учебное пособие	Электронная библиотека	Москва: Национальный Открытый Университет «ИНТУИТ», 2016
Л2.3	Доррер Г. А.	Методы и системы принятия решений: учебное пособие	Электронная библиотека	Красноярск: Сибирский федеральный университет (СФУ), 2016
Л2.4	Целых А. Н., Целых Л. А., Барковский С. А.	Адаптивные информационные системы для поддержки принятия решений: монография	Электронная библиотека	Ростов-на-Дону, Таганрог: Южный федеральный университет, 2018
Л2.5	Белинский А. В.	Квантовые измерения: учебное пособие	Электронная библиотека	Москва: БИНОМ. Лаборатория знаний, 2015
Л2.6	Вишняков Я. Д., Радаев Н. Н.	Общая теория рисков: учеб. пособие для студ. вузов, обуч. по спец. "Менеджмент организации"	Библиотека МИСиС	М.: ACADEMIA, 2007
Л2.7	Адигамов Аркадий Энгелевич, Макаров Петр Витальевич, Семенова Наталья Вячеславовна	Элементы теории графов и оптимизация на сетях	Библиотека МИСиС	, 2009



6.1.3. Методические разработки				
	Авторы, составители	Заглавие	Библиотека	Издательство, год
ЛЗ.1	Макаревич О. Б., Бабенко Л. К., Шилов А. К., Коваленко А. В.	Основы защищенного делопроизводства: по курсу Технология защищенного документооборота: методическое пособие	Электронная библиотека	Таганрог: Издательство ТРТУ, 2000
ЛЗ.2	Киселева И. А.	Моделирование рисков ситуаций: учебно- методический комплекс	Электронная библиотека	Москва: Евразийский открытый институт, 2011
ЛЗ.3	Олейников С. Я., Бочаров С. А., Иванов А. А.	Риск-менеджмент: учебно- методический комплекс	Электронная библиотека	Москва: Евразийский открытый институт, 2011
ЛЗ.4	Минин И. В., Минин О. В.	Защита конфиденциальной информации при электронном документообороте: учебное пособие	Электронная библиотека	Новосибирск: Новосибирский государственный технический университет, 2011
ЛЗ.5	Векилов Юрий Хоренович, Кузьмин Юрий Михайлович, Кадышев Або Ефимович	Теоретическая физика: Разд.: Квантовая механика: Учеб. пособие для практ. занятий для студентов спец. 0406, 0629, 0606	Библиотека МИСиС	М.: Учеба, 1981
ЛЗ.6	Бахаров Леонид Ефимович	Информационная безопасность и защита информации (разделы криптография и стеганография) (N 3854): практикум	Электронная библиотека	М.: [МИСиС], 2019
ЛЗ.7	Петров Андрей Евгеньевич	Математические модели принятия решений (N 3092): учебно-метод. пособие	Электронная библиотека	М.: [МИСиС], 2018
6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э1	Курс "Современные технологии защиты информации" в ЭОИС Canvas. Режим доступа - URL: <a href="https://lms.misis.ru/login/canvas">https://lms.misis.ru/login/canvas</a> ( дата обращения 06.08.23)		<a href="https://lms.misis.ru/login/canvas">https://lms.misis.ru/login/canvas</a>	
Э2	Официальный сайт Федеральной службы РФ по таможенному и экспортному контролю. Режим доступа URL: <a href="https://fstec.ru/">https://fstec.ru/</a> (дата обращения 01.09.2023).		<a href="https://fstec.ru/">https://fstec.ru/</a>	
6.3 Перечень программного обеспечения				
П.1	Win Pro 10 32-bit/64-bit			
П.2	LMS Canvas			
П.3	MS Teams			
П.4	WinRAR			
6.4. Перечень информационных справочных систем и профессиональных баз данных				
И.1	1. Электронно-библиотечная система "Лань" ( <a href="https://e.lanbook.com">https://e.lanbook.com</a> )			
И.2	2. ScienceDirect - база полнотекстовых научных журналов и книг издательства Elsevier ( <a href="https://www.sciencedirect.com">https://www.sciencedirect.com</a> )			
И.3	3. Scopus - единая реферативная база данных научных публикаций ( <a href="https://www.scopus.com">https://www.scopus.com</a> )			
7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ				
Ауд.		Назначение	Оснащение	

Б-734	Лекционная аудитория	комплект учебной мебели на 140 мест для обучающихся, рабочее место преподавателя, мультимедийное оборудование, ноутбук с доступом к ИТС «Интернет», ЭИОС университета через личный кабинет на платформе LMS Canvas, лицензионные программы MS Office, MS Teams, ESET Antivirus и технические средства обучения, служащие для предоставления информации большой аудитории.
Б-835	Учебная аудитория	комплект учебной мебели на 36 мест для обучающихся, мультимедийное оборудование, магнитно-маркерная доска, веб-камера, рабочее место преподавателя, ПК с доступом к ИТС «Интернет», ЭИОС университета через личный кабинет на платформе LMS Canvas, лицензионные программы MS Office, MS Teams, ESET Antivirus.
Читальный зал электронных изданий	Аудитория для самостоятельной работы	комплект учебной мебели на 55 мест для обучающихся, 50 ПК с доступом к ИТС «Интернет», ЭИОС университета через личный кабинет на платформе LMS Canvas, лицензионные программы MS Office, MS Teams, ESET Antivirus.

#### 8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

Дисциплина относится к точным наукам и требует значительного объема самостоятельной работы. Отдельные учебные вопросы выносятся на самостоятельную проработку и контролируются посредством текущей аттестации. Качественное освоение дисциплины возможно только при систематической самостоятельной работе. Курсовая работа проводится с широким использованием компьютерных программ, как для выполнения, так и для оформления работы. Практические работы выполняются с помощью компьютерных программ имитационного моделирования. Так как ситуация в сфере информационной безопасности непрерывно изменяется, кроме рекомендованной литературы, обучающимся следует активно использовать материалы публикаций в сборниках и журналах, сети интернет и социальных сетей, затрагивающие вопросы защиты информации. Приветствуется также посещение студентами специализированных выставок по направлению информационной безопасности и защиты информации с тем, чтобы сформировать наиболее целостное и актуальное представление об изучаемой дисциплине.