КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Форма промежуточной аттестации: экзамен

2025

Рабочая программа по дисциплине «Защищенные информационные системы» по специальности 10.05.01 Компьютерная безопасность, специализации «Разработка защищенного программного обеспечения», составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.01 Компьютерная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от «26» ноября 2020 г. № 1459, профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. № 533н, профессионального стандарта 06.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. №525н.

Рабочая программа:

обсуждена и рекомендована к утверждению решением кафедры естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

одобрена Научно-методическим советом Казанского кооперативного института (филиала) от 2 апреля 2025 г., протокол № 3

СОДЕРЖАНИЕ

1. Цель и задачи освоения дисциплины 4
2. Место дисциплины в структуре образовательной программы 4
3. Перечень планируемых результатов обучения по дисциплине 5
4. Объем дисциплины и виды учебной работы 6
5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий 7
5.1. Содержание дисциплины 7
5.2. Разделы, темы дисциплины и виды занятий 8
6. Практические занятия 10
7. Лабораторные работы 10
8. Примерная тематика курсовых работ (проектов) 11
9. Самостоятельная работа студента 11
10. Оценивание результатов обучения и уровня сформированности компетенций 13
11. Учебно-методическое обеспечение дисциплины 13
12. Перечень программного обеспечения, профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины 15
13. Материально–техническое обеспечение дисциплины 15
Обновление рабочей программы дисциплины (модуля) 17

1. Цель и задачи освоения дисциплины

Целью преподавания и изучения дисциплины «Защищенные информационные системы» является формирование у обучающихся фундаментальных и прикладных знаний в области основ защиты информации в информационных системах, а также формирование умений, навыков и компетенций по применению технологий, методов и средств защиты информации в информационных системах.

Задачами дисциплины являются: изучение основных понятий и методов защиты информации; изучение принципов построения защищенных информационных систем; ознакомление с уязвимостями, угрозами информационных систем и видами деструктивного воздействия, характерными для современных информационных систем; изучение подходов и методов обеспечения информационной безопасности информационных систем.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Физические основы защиты информации» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» основной образовательной программы – программы специалитета по специальности 10.05.01 Компьютерная безопасность специализация «Разработка защищенного программного обеспечения».

Код компетенции	Предшествующие дисциплины (модули), практики	Изучаемые в текущем семестре дисциплины (модули), практики	Последующие дисциплины (модули), практики
ОПК-6, ОПК- 9.1	Автоматизация тестирования ПО	Защищенные информационные системы Защита информации от утечки по техническим каналам	-

3. Перечень планируемых результатов обучения по дисциплине

Изучение дисциплины направлено на формирование у обучающихся компетенций.

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1. Применяет в профессиональной деятельности знания нормативной правовой базы при организации защиты информации ограниченного доступа в компьютерных системах и сетях	Знать: нормативные правовые акты и методические документы, регламентирующие организацию защиты информации ограниченного доступа в компьютерных системах и сетях. Умеет: Применять в профессиональной деятельности знания нормативных и правовых актов и нормативных методических документов при организации защиты информации ограниченного доступа в информационных системах Владеть: навыками практического применения положений нормативных актов и методических рекомендаций для обеспечения информационной безопасности организаций.
	ОПК-6.2 Демонстрирует умения организации физической защиты объекта информатизации	Знать: основные угрозы объекту информатизации и меры физической защиты, используемые для минимизации этих угроз. Уметь: проектировать систему физической защиты объекта информатизации, включающую инженерно-технические средства охраны и контроль доступа. Владеет: умениями организации физической защиты информационной системы и обоснованного выбора инженерно-технических средств защиты
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего	ОПК-9.1. Демонстрирует умение решать задачи профессиональной деятельности с учетом текущего состояния и	Знать: современное состояние и перспективные направления развития компьютерных сетей, протоколы и топологии, влияющие на решение профессиональных

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	тенденций развития компьютерных сетей	задач. Умеет: решать задачи защиты информации в информационных системах с учетом текущего состояния и тенденций развития компьютерных сетей. Владеть: навыками выбора оптимальных архитектур и протоколов для построения высокопроизводительных и надежных сетей в профессиональной деятельности.
	ОПК-9.2.Демонстрирует умение решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития сетей и систем передачи информации	Знать: текущее состояние и перспективы развития сетей и систем передачи информации, ключевые технологии и протоколы. Уметь: решать задачи защиты информации в информационных системах с учетом текущего состояния и тенденций развития сетей и систем передачи информации Владеть: навыками эффективного использования современных технологий и стандартов передачи информации для успешной реализации профессиональных задач.

4. Объем дисциплины и виды учебной работы

Объем дисциплины и виды учебной работы в академических часах с выделением объема контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся

очная форма обучения

Вид учебной деятельности	ак.часов	
	Всего	По семестрам
		9
1. Контактная работа обучающихся с преподавателем:	69	69
Аудиторные занятия, часов всего, в том числе:	68	68
• занятия лекционного типа	34	34
• занятия семинарского типа:	34	34
практические занятия	-	-

лабораторные занятия		34	34
в том числе занятия в форме практической подготовки		-	-
Консультации		0,5	0,5
Контактные часы на аттестацию в период экзаменационных сессий		0,5	0,5
2. Самостоятельная работа студентов всего, в том числе		39	39
- подготовка курсовой работы		-	-
- проработка учебного (теоретического) материала		18	18
- выполнение домашних заданий по практическим занятиям		18	18
3. Подготовка к экзамену		36	36
Промежуточная аттестация: экзамен		-	-
ИТОГО:	часов	144	144
общая трудоемкость	зач. ед.	4	4

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Понятие и особенности функционирования информационной системы (ИС). Архитектуры, применяемые в информационных системах.

Понятие информационной системы, основные компоненты информационной системы. Виды информационных систем. Особенности различных архитектур информационных систем. Уровни организации архитектур информационных систем. Особенности распределённых информационных систем. Структура и состав информационной системы. Описание физических, функциональных, технологических и логических взаимосвязей

Тема 2. Основные аспекты построения защищенных информационных систем

Регулирование ответственности нарушений информационной безопасности. Программа информационной безопасности. Контроль деятельности в области безопасности. Модели представления информационной защиты. Формирование требований к системе информационной безопасности. Этапы обеспечения информационной безопасности.

Тема 3. Определение уровня защищенности данных в информационной системе

Определение типа угроз безопасности информации. Определение категории обрабатываемых данных. Определение количества субъектов данных.

Определение уровня защищенности данных. Определение класса

информационной системы. Оценка степени возможного ущерба. Определение класса защищенности информационной системы.

Тема 4. Перечень потенциальных источников атак и определение их возможностей (модель нарушителя)

Категория лиц, рассматриваемых и не рассматриваемых в качестве нарушителей. Обобщенные возможности нарушителя.

Уточненные возможности нарушителя. Актуальность использования (применения) возможностей нарушителя для построения и реализации атак. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности данных.

Тема 5. Описание угроз безопасности информации (модель угроз безопасности информации)

Определение перечня угроз безопасности информации, возможных с учетом потенциала нарушителя. Определение перечня угроз безопасности информации, возможных с учетом применяемых технологий. Определение исходной защищенности информационной системы. Определение частоты (вероятности) реализации угроз. Определение объема негативных последствий. Способы реализации угроз безопасности информации. Возможные уязвимости информационной системы.

Тема 6. Методы выбора системы защиты информации

Классификация методов выбора систем защиты информации. Метод анализа иерархий. Метод парных сравнений альтернатив.

Многокритериальный выбор в иерархических структурах с множеством различных альтернатив под критериями. Методы принятия решений, основанные на исследовании операций.

Сопоставление угроз и методов и средств их устранения. Игровые стратегии выбора системы защиты информации

5.2. Разделы, темы дисциплины и виды занятий

очная форма обучения

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в часах)			Индикаторы достижения компетенций
		занятия лекционного типа	занятия семинарского типа / из них в форме практической подготовки (лабораторные работы)	самос-тоятельная работа	

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в часах)			Индикаторы достижения компетенций
		занятия лекционного типа	занятия семинарского типа / из них в форме практической подготовки (лабораторные работы)	самос-тоятельная работа	
1	Понятие и особенности функционирования информационной системы. Архитектуры, применяемые в информационных системах.	6	6/6	6	ОПК-6, ОПК-6.1, ОПК-6.2, ОПК-9, ОПК-9.1, ОПК-9,2
2	Основные аспекты построения защищенных информационных систем	6	6/6	6	ОПК-6, ОПК-6.1, ОПК-6.2, ОПК-9, ОПК-9.1, ОПК-9,2
3	Определение уровня защищенности данных в информационной системе	6	6/6	6	ОПК-6, ОПК-6.1, ОПК-6.2, ОПК-9, ОПК-9.1, ОПК-9,2
4	Перечень потенциальных источников атак и определение их возможностей (модель нарушителя)	6	6/6	6	ОПК-6, ОПК-6.1, ОПК-6.2, ОПК-9, ОПК-9.1, ОПК-9,2
5	Описание угроз безопасности информации (модель угроз безопасности информации)	6	6/6	6	ОПК-6, ОПК-6.1, ОПК-6.2, ОПК-9, ОПК-9.1, ОПК-9,2
6	Методы выбора системы защиты информации	4	4/4	9	ОПК-6, ОПК-6.1, ОПК-6.2, ОПК-9, ОПК-9.1, ОПК-9,2
	Всего	**34**	**34/34**	**39**	

6. Практические занятия

Практические занятия не предусмотрены.

7. Лабораторные работы

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
1.	Понятие и особенности функционирования информационной системы. Архитектуры, применяемые в информационных системах.	Определение уровня исходной защищённости Определение типа актуальной угрозы	6
2.	Основные аспекты построения защищенных информационных систем	Формирование требований к системе информационной безопасности. Определение частоты (вероятности) реализации рассматриваемой угрозы Определение коэффициента реализуемости угрозы и возможности реализации	6
3.	Определение уровня защищенности данных в информационной системе	Определение типа угроз безопасности информации. Определение категории обрабатываемых данных. Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах	6
4.	Перечень потенциальных источников атак и определение их возможностей (модель нарушителя)	Определение категории лиц рассматриваемых и не рассматриваемых в качестве нарушителей. Уточнение возможности нарушителя. Создание модели вероятного нарушителя Разработка нормативных правовых актов, определяющих угрозы безопасности данных ИС организации.	6
5.	Описание угроз безопасности информации (модель угроз безопасности информации)	Определение перечня угроз безопасности информации, возможных с учетом потенциала нарушителя и с учетом применяемых технологий. Определение исходной защищенности информационной системы. Определение частоты (вероятности) реализации угроз. Составление модели угроз безопасности информационной системы	6
6.	Методы выбора системы защиты информации.	Методы выбора систем защиты информации: Метод анализа иерархий. Метод парных сравнений альтернатив. Многокритериальный выбор в иерархических структурах с множеством различных альтернатив. Определение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах	4

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
	Всего		**34**

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Защищенные информационные системы» направлена на:

– освоение нормативных правовых актов и учебной литературы, необходимых для освоения дисциплины;

– самостоятельный поиск информации в Интернете и других источниках;

– выполнение домашних заданий по практическим занятиям;

– подготовку к зачету.

Краткие рекомендации по выполнению самостоятельной работы:

Успешное усвоение дисциплины предполагает большой, упорный, серьезный, систематический труд студентов. Важнейшая его составная часть – выполнение разных видов самостоятельной работы.

1. **Составление тематического конспекта** на основе изученной основной и дополнительной учебной литературы. В тематическом конспекте за основу берется содержание темы, вопросы для обсуждения.

Этапы работы.

1.1 Конспектирование делается только после того, как прочитан или усвоен материал для конспектирования.

1.2. Необходимо мысленно или письменно составить план конспекта. По этому плану и будет строиться конспект далее.

1.3. Составление самого конспекта. Можно сказать, что конспект – это расширенные тезисы, дополненные рассуждениями и доказательствами, содержащимися в материалах для конспекта, а также собственными мыслями и положениями составителя конспекта.

Писать конспект рекомендуется четко и разборчиво. В конспекте можно выделять места текста в зависимости от их значимости. Для этого применяются различного размера буквы, подчеркивания, замечания на полях.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Зачетно-экзаменационные материалыдля промежуточной

аттестации (зачет)

1.Понятие информационной системы, основные компоненты информационной системы.
2.Виды информационных систем. Особенности различных архитектур информационных систем.
3.Уровни организации архитектур информационных систем. Особенности распределённых информационных систем.
4.Структура и состав информационной системы. Описание физических, функциональных, технологических и логических взаимосвязей
5.Регулирование ответственности нарушений информационной безопасности.
6.Программа информационной безопасности.
7.Контроль деятельности в области безопасности.
8.Модели представления информационной защиты.
9.Формирование требований к системе информационной безопасности.
10.Этапы обеспечения информационной безопасности.
11.Определение типа угроз безопасности информации.
12.Определение категории обрабатываемых данных.
13.Определение количества субъектов данных.
14.Определение уровня защищенности данных.
15.Определение класса информационной системы.
16.Оценка степени возможного ущерба.
17.Определение класса защищенности информационной системы.
18.Категория лиц, рассматриваемых и не рассматриваемых в качестве нарушителей.
19.Обобщенные возможности нарушителя. Уточненные возможности нарушителя.
20.Актуальность использования (применения) возможностей нарушителя для построения и реализации атак.
21.Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности данных.
22.Определение перечня угроз безопасности информации, возможных с учетом потенциала нарушителя.
23.Определение перечня угроз безопасности информации, возможных с учетом применяемых технологий.
24.Определение исходной защищенности информационной системы.
25.Определение частоты (вероятности) реализации угроз.
26.Определение объема негативных последствий.
27.Способы реализации угроз безопасности информации.
28.Возможные уязвимости информационной системы.
29.Классификация методов выбора систем защиты информации.
30.Метод анализа иерархий.
31.Метод парных сравнений альтернатив.
32.Многокритериальный выбор в иерархических структурах с множеством

различных альтернатив под критериями.
33.Методы принятия решений, основанные на исследовании операций.
34.Сопоставление угроз и методов и средств их устранения.
35.Игровые стратегии выбора системы защиты информации
Код контролируемой компетенции: ОПК-6; ОПК-9.

4.2.2Образцы билетов
Билет №1
1.Понятие информационной системы, основные компоненты информационной системы.
2.Определение перечня угроз безопасности информации, возможных с учетом потенциала нарушителя.

Билет №2
1.Модели представления информационной защиты.
2.Определение исходной защищенности информационной системы.

10. Оценивание результатов обучения и уровня сформированности компетенций

Оценивание результатов обучения по дисциплине и уровня сформированности компетенций (части компетенции) осуществляется в рамках текущего контроля успеваемости и промежуточной аттестации в соответствии с оценочными материалами.

11. Учебно-методическое обеспечение дисциплины

Основная литература:

Основная литература

1. Мошак, Н. Н. Защищенные информационные системы : учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020.

— 216 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180099 — Режим доступа: для авториз. пользователей.

2. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507- 46010-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/293009 — Режим доступа: для авториз. пользователей.

3. Парфёнов, Ю. П. Средства управления и защиты информационных ресурсов автоматизированных систем : учебное пособие / Ю. П. Парфёнов. — 2-е изд. — Москва : ФЛИНТА, 2022. — 120 с. — ISBN 978-5-9765-5016-2. — Текст :

электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/231707 — Режим доступа: для авториз. пользователей.

4. Программно-аппаратные средства защиты информационных систем : учебное пособие

: в 3 частях / В. А. Гриднев, Ю. А. Губсков, А. С. Дерябин, А. В. Яковлев. — Тамбов : ТГТУ, 2022 — Часть 1 — 2022. — 77 с. — ISBN 978-5-8265-2467-1. — Текст :

электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/355133 — Режим доступа: для авториз. пользователей.

Дополнительная литература

1. Нестандартные методы защиты информации : учебное пособие / составители В. П. Пашинцев, А. В. Ляхов. — Ставрополь : СКФУ, 2016. — 196 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155239. — Режим доступа: для авториз. пользователей.

2. Щеглов, А. Ю. Математические модели и методы формального проектирования систем защиты информационных систем : учебное пособие / А. Ю. Щеглов, К. А. Щеглов.—Санкт-Петербург : НИУ ИТМО, 2015. — 93 с. — Текст : электронный // Лань : электроннобиблиотечная система. — URL: https://e.lanbook.com/book/70897 — Режим доступа: для авториз. пользователей.

5.3 Периодическая литература

1. Базы данных компании «Ист Вью» http://dlib.eastview.com
2. Электронная библиотека GREBENNIKON.RU https://grebennikon.ru/

Электронные библиотечные системы (ЭБС) и электронные образовательные ресурсы

1. Электронно-библиотечная система ZNANIUM https:// www.znanium.com
2. Универсальная справочно-информационная полнотекстовая база данных периодических изданий «East View» (ИВИС) https://dlib.eastview.com/
3. Электронно-библиотечная система «BOOK.ru» www.book.ru
4. Электронно-библиотечная система «IPRbooks» http://www.iprbookshop.ru/
5. ЭБС «Национальный цифровой ресурс «Руконт» https://lib.rucont.ru/search
6. Образовательная платформа ЮРАЙТ http://www.urait.ru

Электронный каталог Университета – Автоматизированная информационная библиотечная система (АИБС «МегаПро»)

12. Перечень программного обеспечения, профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины

Лицензионное программное обеспечение, в том числе отечественного производства:

– DsktpEdu ALNG LicSARk OLV F1 1Y Acdmc Ent (MS Windows) (подписка на ПО).

Свободно распространяемое программное обеспечение, в том числе отечественного производства:

– 7-Zip (свободный файловый архиватор с высокой степенью сжатия данных) (отечественное ПО).

– FastStone Image Viewer (программа для просмотра изображений в Microsoft Windows (лицензия бесплатного программного обеспечения)).

– Foxit Reader (Бесплатное прикладное программное обеспечение для просмотра электронных документов в стандарте PDF (лицензия бесплатного программного обеспечения)).

– Indigo (система программ для создания и проведения компьютерного тестирования знаний).

– Google Crome, ЯндексБраузер (браузер).

– Adobe Acrobat Reader DC (• ПО для просмотра, печати и комментирования документов в формате PDF)

– Visual Studio Code (интегрированная среда разработки программного обеспечения)

Профессиональные базы данных не используются.

Информационные справочные системы:

– СПС КонсультантПлюс. Компьютерная справочная правовая система, широко используется учеными, студентами и преподавателями (подписка на ПО)

Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронно-библиотечной

13. Материально–техническое обеспечение дисциплины

Образовательный процесс обеспечен учебными аудиториями для проведения учебных занятий, а именно для проведения занятий лекционного типа, лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещениями для самостоятельной работы студентов.

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Рабочее место преподавателя (стол, стул), рабочие места обучающихся,

доска для написания мелом, кафедра.

Технические средства обучения: персональный компьютер-1, мультимедийное оборудование (проектор, проекционный экран) - 1

Учебная аудитория для проведения лабораторных занятий. Аудитория информационных технологий

Рабочее место преподавателя (стол, стул), рабочие места обучающихся:

Технические средства обучения: персональный компьютер с подключением к сети «Интернет» - 15, сетевое оборудование.

Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду института.

Рабочие места обучающихся.

Технические средства обучения: персональный компьютер - 13.

Учебные аудитории соответствуют действующим противопожарным правилам и нормам, укомплектованы учебной мебелью.

Обновление рабочей программы дисциплины (модуля)

Наименование раздела рабочей программы, в который внесены изменения

(измененное содержание раздела)

обсуждено и рекомендовано к утверждению решением кафедры наименование кафедры
от ___ _____ 20_ г., протокол № ___

одобрено Научно-методическим советом _____ от ___ _____ 20__ г., протокол №____