РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность распределённых информационных систем (наименование дисциплины (модуля) по УП)

Закреплена за кафедрой: систем информационной безопасности

Направление подготовки (специальности):

10.05.03 Информационная безопасности телекоммуникационных систем

(код, наименование)

Профиль: Системы подвижной цифровой защищенной связи

(название профиля по УП)

Часов по УП: 108**; Часов по РПД:** 108**;**

Часов по УП (без учета часов на экзамены): 108**; Часов по РПД:** 108**;**

Часов на интерактивные формы (ИФ) обучения по УП: 54

Часов на интерактивные формы (ИФ) обучения по РПД: 54

Часов на самостоятельную работу по УП: 36 (33%);

Часов на самостоятельную работу по РПД: 36 (33%)

Общая трудоемкость в ЗЕТ: 3**;**

Виды контроля в семестрах (на курсах): Экзамены - 1; Зачеты - 0; Курсовые проекты - 1; Курсовые работы - 0.

Форма обучения: очная**;**

Срок обучения: нормативный**.**

Распределение часов дисциплины по семестрам

Вид занятий	**№ семестров, число учебных недель в семестрах**									
	7 / 18		8 / 20		9 / 18		А / 18		Итого	
	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД
Лекции							36	36	36	36
Лабораторные										
Практические							36	36	36	36
Ауд. занятия							72	72	72	72
Сам. работа							36	36	36	36
Итого							108	108	108	108

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	**Цель изучения дисциплины** – обучить студентов выявлять и противодействовать атакам вредоносных программ и злоумышленников в распределенных системах обработки информации.
1.2	**Для достижения цели ставятся задачи:**
1.2.1	изучение методологии обнаружения уязвимостей распределенной информационной системы;
1.2.2	освоение методологии системного анализа и синтеза структуры, состава систем защиты распределенной информационной системы;
1.2.3	изучение методологии контроля эффективности системы безопасности распределенной информационной системы.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

Цикл (раздел) ООП: С3	код дисциплины в УП: С3.Б.18
2.1 Требования к предварительной подготовке обучающегося	
С2.Б.4	Теория вероятностей и математическая статистика
С2.Б.5	Математическая логика и теория алгоритмов
С2.Б.6	Теория информации
С2.Б.10	Теория графов и её приложения
С2.В.ОД.1	Физические основы защиты информации
С2.В.ОД.2	Математические основы риск-анализа
С3.Б.2	Языки программирования
С3.Б.3	Технологии и методы программирования
С3.Б.7	Безопасность систем баз данных
С3.Б.9	Основы информационной безопасности
С3.Б.12	Сети и системы передачи информации
2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее	
С3.Б.11	Техническая защита информации
С3.Б.14	Программно-аппаратные средства обеспечения информационной безопасности
С3.Б.15	Разработка и эксплуатация защищенных автоматизированных систем
С3.Б.16	Управление информационной безопасностью
С3.Б.19	Методы проектирования защищённых распределённых информационных систем
С3.Б.20	Технология построения защищённых распределённых приложений используются обучаемыми при выполнении дипломных работ

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-15	способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем
ПСК-7.2	способность разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах
ПСК-7.3	способность проводить анализ рисков информационной безопасности в распределенных информационных системах
ПСК-7.4	способность разрабатывать и руководить разработкой политики безопасности распределенных информационных систем
ПСК-7.5	способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем
ПСК-7.6	способность проводить удаленное администрирование операционных систем в распределенных информационных системах
ПСК-7.7	способность проводить удаленное администрирование систем баз данных в распределенных информационных системах
ПСК-7.8	способность координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации

Требования к результатам освоения дисциплины

В результате освоения дисциплины обучающийся должен обладать знаниями, умениями и навыками, приведенными в таблице.

Код компетенции по ФГОС ВПО или ООП	Содержание компетенции (или ее части)	В результате изучения дисциплины обучающиеся должны:		
		Знать	Уметь	Владеть
ПК-15	способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем	научные основы и методику работы с источниками информации; современные средства и методы обеспечения безопасности распределенных систем обработки информации	использовать системы поддержки принятия решений при выборе эффективных проектов защиты распределенных систем; применять современные средства и методы мониторинга, технической диагностики средств защиты, оценки эффективности информационной безопасности защищенных распределенных систем	методикой контроля информационной целостности в распределенной систем обработки информации; методами концептуального проектирования защищенных распределенных систем
ПСК-7.2	способность разрабатывать модели угроз и модели	методы и средства обнаружения уязвимостей распределенной информацион-	применять современные программные инструментарии	профессиональной терминологией;

	нарушителя информационной безопасности в распределенных информационных системах	ной системы; перспективные направления развития средств и комплексов защиты распределенных систем обработки информации; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения защиты информации в распределенных информационных системах	для моделирования угроз распределенным информационным системам	методами разработки моделей угроз и модели нарушителя информационной безопасности в распределенных информационных системах
ПСК-7.3	способность проводить анализ рисков информационной безопасности в распределенных информационных системах	основные причины и особенности современных информационных угроз; методы и средства обнаружения атак на ресурсы распределенной информационной системы;	классифицировать угрозы информационной безопасности с целью создания эффективной защиты распределенной информационной системы от угроз; проводить анализ и оценку рисков информационной безопасности	средствами анализа защищенности и обнаружения/предотвращения вторжений;
ПСК-7.4	способность разрабатывать и руководить разработкой политики безопасности распределенных информационных систем	проблемы передачи информации и их решения; методы и средства противодействия атакам на ресурсы распределенной информационной системы	пользоваться научно - технической литературой и справочной информацией по информационной безопасности; эксплуатировать средства обеспечения ИБ распределенных систем обработки информации; разрабатывать организационно-распорядительные и нормативно-технические документы регулирующие обеспечение информационной безопасности в организации. разрабатывать предложения по выбору корректирующих	навыками безопасного использования технических средств в профессиональной деятельности

			действий по предотвращению инцидентов;	
ПСК-7.5	способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем	современные средства и методы мониторинга, технической диагностики средств защиты, оценки эффективности информационной безопасности защищенных распределенных систем	организовывать и проводить внутренний аудит; эксплуатировать средства обеспечения ИБ распределенных систем обработки информации;	методами оценки текущего уровня защищенной распределенной системы: методами и средствами контроля обеспечения эффективности и непрерывности защиты информации
ПСК-7.6	способность проводить удаленное администрирование операционных систем в распределенных информационных системах	архитектуру средств информатизации; методы обеспечения защиты на объекте информатизации	производить защиту от атак на ресурсы распределенной информационной системы; эксплуатировать средства обеспечения ИБ распределенных систем обработки информации;	методами устранения уязвимостей в коде; методами и средствами мониторинга и удаленного управления операционной системой
ПСК-7.7	способность проводить удаленное администрирование систем баз данных в распределенных информационных системах	методику организации баз данных; методы оценки рисков информации; методы удаленного контроля и мониторинга баз данных	производить защиту от атак на ресурсы распределенной информационной системы; эксплуатировать средства обеспечения ИБ распределенных систем обработки информации;	средствами борьбы с атаками злоумышленников на ресурсы серверов баз данных;
ПСК-7.8	способность координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации	мероприятия по обеспечению безопасности распределенных информационных систем; методы организации работы по обеспечению защиты информации в распределенных информационных системах; законодательные акты, отечественные и международные	разрабатывать локальные политики безопасности распределенн ых систем обработки информации; эксплуатировать средства обеспечения ИБ распределенных систем обработки информации; управлять инцидентами	навыками безопасного использования технических средств в профессиональной деятельности; научными основами и современными методиками обеспечения безо-

		стандарты по защите информации		пасности распределенной информационной системы

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ П./п	Наименование раздела дисциплины	Семестр	Неделя семестра	Вид учебной нагрузки и их трудоемкость в часах				
				Лекции	Практические занятия	Лабораторные. работы	СРС	Всего часов
1	Принципы проектирования архитектуры и структуры распределенных систем обработки информации	7	1-3	6	6		6	18
2	Атаки на интрасети и интернет-сети	7	3-7	6	6		6	18
3	Основы построения систем обнаружения вторжений	7	8-14	16	16		16	48
4	Контроль эффективности системы безопасности распределенной информационной системы	7	15-18	8	8		8	24
	Итого			36	36		36	108

4.1 Лекции

Неделя семестра	Тема и содержание лекции	Объем часов	В том числе, в интерактивной форме (ИФ)
7 семестр		**36**	2,5
Принципы проектирования архитектуры и структуры распределенных систем обработки информации		**6**	0,5
1	**Введение** Основные понятия. Распределенная информационная система, ее функции. Полностью неоднородные, частично однородные и однородные распределенные системы обработки данных. Классификация распределенных информационных систем по архитектурным особенностям и по степени распределенности. Способы организации взаимодействия между ЭВМ. Характеристики распределенной информационной системы. Технология «клиент-сервер». Серверы приложений и прикладные протоколы. Представление данных в информационных системах.	2	0
2-3	**Архитектура распределенной информационной системы**	4	0,5

	Логическая, физическая и программная структуры распределенной информационной системы. Назначение и функции элементов этих структур. Концепция взаимодействия открытых систем. Иерархия системы обработки данных: уровень архитектуры системы обработки данных, среда для конечного пользователя и инструментарий прикладного программиста, операционная система, оборудование. Объектно-ориентированные системы. Свойства открытых систем и объектно-ориентированных систем программирования		
Атаки на интрасети и интернет-сети		**6**	0,5
4	**Интрасети и Интернет-сети** Локальные сети LAN и глобальные (региональные) сети WAN, сетевые комплексы или объединенные сети. Термины Карта Сетевого Интерфейса, Физический Порт, Интерфейсы. Стандартные обозначения компонентов сетей. Понятие «интрасеть». Различие интрасети и Интернет-сети. Возможности и предоставляемые услуги.	2	0,25
5	**Порядок предоставления доступа** Виды доступа. Обязанности пользователей. Права и обязанности управления информатизации по администрированию интрасети. *Самостоятельное изучение.* Абсолютно упругий и неупругий удар.	2	0
6	**Атаки на интрасети и Интернет-сети** Классификация типов удаленных атак на интрасети по степени риска (Risk Factor), по типу атаки (Attack Type), по подверженному данной атаке программному обеспечению (Platforms Affected). Анализ сетевого трафика. Подмена доверенного объекта. Введение ложного объекта компьютерной сети. Отказ в обслуживании (DoS). Сканирование компьютерных сетей. Сети botnet (Blue Coat Security Labs) *Самостоятельное изучение.* Эволюция угроз.	2	0,25
7	**Классификация угроз безопасности Web-приложений** Аутентификация (Authentication). Авторизация (Authorization). Атаки на клиентов (Client-side Attacks). Выполнение кода (Command Execution). Разглашение информации (Information Disclosure). Логические атаки (Logical Attacks).	2	0
Основы построения систем обнаружения вторжений		**16**	1
8	**Системы обнаружения вторжений** Понятие «Система обнаружения вторжений». Функции системы обнаружения вторжений. Виды систем обнаружения вторжений. Пассивные и активные системы обнаружения вторжений. Основные компоненты системы обнаружения вторжений: датчики (сенсоры) и анализаторы.	2	0,25
9	**Принципы функционирования систем обнаружения вторжений** Структура современных систем обнаружения вторжений. Сущность и функции ее подсистем: подсистемы сбора информации, подсистемы анализа и подсистемы представления данных. Анализ недостатков современных систем обнаружения вторжений.	2	0,25
10	**Требования по безопасности информации** Функциональные требования безопасности для систем обнаружения вторжений. Механизмы защиты. Профили защиты системы обнаружения вторжений. Идентификация профиля защиты. Организация профиля защиты.	2	0

11-13	**Методы обнаружения вторжений** Подходы к защите от типовых удаленных атак на интрасети. Методы обнаружения аномалий: моделирование правил, описательная статистика, нейронные сети, моделирование множества состояний, описательная статистика. Методы обнаружения злоупотреблений: моделирование состояний, экспертные системы, моделирование правил, синтаксический анализ. Методы, основанные на моделировании поведения злоумышленника.	6	0,25
14-15	**Технологии построения систем обнаружения атак** Существующие технологии построения систем обнаружения атак. Технологии обнаружения аномальной деятельности. Статистический анализ компьютерных атак. Анализ систем, использующих сигнатурные методы. Анализ систем, использующих методы поиска аномалий в поведении. Общая оценка современного подхода к обнаружению вторжений. Концепция обнаружения компьютерных угроз	4	0,25
Контроль эффективности системы безопасности распределенной информационной системы		**6**	0,5
16	**Стандарты управления информационной безопасностью** Стандарты ISO/IEC 17799:2002 (BS 7799:2000) – ГОСТ Р ИСО/МЭК 17799 «Управление информационной безопасностью — Информационные технологии» (Information technology — Information security management»)	2	0
17	**Повышение эффективности систем обнаружения атак — интегральный подход** Сценарий атаки. Фазы атаки. Схема интегрального обнаружения компьютерных атак. Эффективность проверки правил в системах обнаружения сетевых атак. Требования доверия к безопасности системы обнаружения вторжений. Аудит безопасности. Управление безопасностью.	2	0,25
18	**Администрирование безопасности.** Административные, технические (логические) и физические меры. Администрирование информационной системы в целом. Администрирование сервисов безопасности. Аадминистрирование механизмов безопасности. Обязанности и ответственность администратора. Поддержка безопасности в распределенной системе Типичные проблемы безопасности.	2	0,25
Итого часов		**36**	2,5

4.2 Практические занятия

Неделя семестра	Тема и содержание практического занятия	Объем часов	В том числе, в интерактивной форме (ИФ)	Виды контроля
1 семестр		**36**	**32**	
Принципы проектирования архитектуры и структуры распределенных систем обработки информации		**6**	**4**	
1	Вводное занятие. Входной контроль	2	0	

2	HTML-редактор Dreamweaver MX. Знакомство с интерфейсом программы Dreamweaver. Предварительная настройка Dreamweaver.	2	2	
3	Dreamweaver. Набор и форматирование текста. Работа с таблицами.	2	2	
Атаки на интрасети и интернет-сети		**6**	**6**	
4	Dreamweaver. Вставка графических изображений. Создание гиперссылок. Знакомство со справочной системой.	2	2	
5	Dreamweaver. Создание документа с фреймами	2	2	
6	Dreamweaver. Создание документа с формами	2	2	
Основы построения систем обнаружения вторжений		**16**	**16**	
7	Использование программы Dr. WEB	2	2	
8	Использование программы Dr. WEB в режиме графического интерфейса	2	2	
9-10	Изучение JavaScript. Создание кнопки	4	4	
11-12	Изучение JavaScript. Бегущая строка	4	4	
13-14	Изучение JavaScript. Горизонтальное меню.	4	4	
Контроль эффективности системы безопасности распределенной информационной системы		**8**	**8**	
15-16	Изучение JavaScript. Показ баннера.	4	4	
17	Настройка для Microsoft Internet Explorer для обеспечения безопасности использования WWW	2	2	
18	**Контрольная работа**	2	0	Контр. раб.
Итого часов		**36**	**32**	

4.3 Лабораторные работы

Не предусмотрены

4.4 Самостоятельная работа студента (СРС)

Неделя семестра	Содержание СРС	Виды контроля	Объем часов
7 семестр		**Экзамен**	**36**
2	Подготовка к практическому занятию	проверка домашнего задания	1
3	Работа с конспектом лекций, с учебником		0,5
	Подготовка к практическому занятию	проверка домашнего задания	1
4	Работа с конспектом лекций, с учебником		0,5
	Подготовка к практическому занятию	проверка домашнего задания	1
5	Работа с конспектом лекций, с учебником	выборочный опрос	0,5
	Подготовка к практическому занятию	проверка домашнего задания	1
	Работа с конспектом лекций, с учебником		0,5
6	Подготовка к практическому занятию	проверка домашнего задания	1
	Подготовка конспекта по теме для самостоятельного изучения	проверка конспекта	0,5
7	Подготовка к практическому занятию	проверка домашнего задания	1

	Подготовка конспекта по теме для самостоятельного изучения	проверка конспекта	0,5
8	Подготовка к практическому занятию	проверка домашнего задания	1
	Подготовка конспекта по теме для самостоятельного изучения	проверка конспекта	0,5
	Подготовка курсового проекта	Проверка проекта	6
9	Работа с конспектом лекций, с учебником		0,5
	Подготовка к практическому занятию	проверка домашнего задания	1
10	Подготовка к практическому занятию	проверка домашнего задания	1
	Работа с конспектом лекций, с учебником		0,5
11	Работа с конспектом лекций, с учебником		0,5
	Подготовка к практическому занятию	проверка домашнего задания	1
12	Подготовка к практическому занятию	проверка домашнего задания	1
	Подготовка конспекта по теме для самостоятельного изучения	проверка конспекта	0,5
13	Работа с конспектом лекций, с учебником		0,5
	Подготовка к практическому занятию	проверка домашнего задания	1
14	Подготовка к практическому занятию	проверка домашнего задания	1
	Подготовка конспекта по теме для самостоятельного изучения	проверка конспекта	0,5
15	Работа с конспектом лекций, с учебником	выборочный опрос	1
	Подготовка к практическому занятию	проверка домашнего задания	0,5
16	Подготовка к практическому занятию	проверка домашнего задания	1
	Работа с конспектом лекций, с учебником		0,5
17	Работа с конспектом лекций, с учебником	выборочный опрос	0,5
	Подготовка к контрольной работе	контр. раб.	1
18	Подготовка к экзамену	экзамен	6,0

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

	В рамках изучения дисциплины предусмотрены следующие образовательные технологии:
5.1	**Информационные лекции**;
5.2	**Практические занятия**: а) **работа в команде (ИФ) -** совместное обсуждение вопросов лекций, домашних заданий, решение творческих задач (метод Делфи); б) проведение контрольных работ;
5.3	**самостоятельная работа студентов**: – изучение теоретического материала, – подготовка к лекциям, практическим занятиям, конспекты, – работа с учебно-методической литературой, – оформление конспектов лекций, – подготовка к текущему контролю успеваемости, к зачету и экзамену; – изучение теоретического материала, – подготовка курсового проекта
5.4	**консультации** по всем вопросам учебной программы.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

6.1	**Контрольные вопросы и задания**
6.1.1	Используемые формы текущего контроля: – контрольная работа; – курсовой проект; – опрос.
6.1.2	Рабочая программа дисциплины обеспечена фондом оценочных средств для проведения входного, текущего контроля и промежуточной аттестации. Фонд включает примерные варианты контрольных работ, вопросы к экзаменам и зачету. Фонд оценочных средств представлен в учебно – методическом комплексе дисциплины.
6.2	**Темы курсового проектирования**
7 семестр	
6.2.1	Проектирование системы информационной безопасности

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

7.1 Рекомендуемая литература				
№ п/п	**Авторы, составители**	**Заглавие**	**Годы издания. Вид издания**	**Обеспеченность**
7.1.1. Основная литература				
7.1.1.1	Таненбаум Э., ван-Стеен М.	Распределенные системы. – СПб.: Питер	2003 печат.	
7.1.1.2	Дуванов А.А.	Web-конструирование. HTML. – СПб.: БХВ-Петербург	2005 печат.	
7.1.1.3	А.П.Курило, С.П.Зефиров, В.Б.Голованов и др. Воробьев А.А.	Аудит информационной безопасности. М.: «БДЦ-пресс»	2006 печат.	
7.1.1.4	В.Ф.Шаньгин	Информационная безопасность компьютерных систем и сетей. М: ИД «ФОРУМ»-ИНФРА-М	2008 Печат.	
7.1.2. Дополнительная литература				
7.1.2.1	Дронов В.А.	Macromedia Dreamweaver 2004. – СПб.: БХВ-Петербург	2004 печат.	
7.1.2.2	Дронов В.А.	PHP, MySQL и Dreamweaver MX 2004. – СПб.: БХВ-Петербург	2005 печат.	
7.1.2.3	Матросов А.В. и др.	HTML 4.0. СПб.: БХВ-Петербург	2004 печат.	
7.1.2.4	Вайк А. и др.	JavaScript. Полное руководство, 4-е издание. М.: Издательский дом «Вильямс», 2004.	2004 печат.	
7.1.2.5	А.А.Малюк, С.В.Пазизин,	Введение в защиту информации в автоматизированных системах. М. – Горячаятлмнмя-Телеком	2001 печат.	
7.1.3 Методические разработки				

7.1.3.1	Хабарова О.С. Бурова С.В. Тураева Т.Л. Пономаренко Е.Н.	Методические указания к аудиторным занятиям и домашним заданиям по физике (Разноуровневые задачи по теме: «Физические основы механики») для студентов всех технических специальностей очной формы обучения	2006 магн. носитель	1
7.1.3.2	Хабарова О.С. Бурова С.В. Тураева Т.Л.	Методические указания к практическим занятиям и домашним заданиям по физике (Разноуровневые задачи по теме: «Молекулярная физика. Термодинамика») для студентов всех технических специальностей очной формы обучения	2006 печат.	1
7.1.3.3	Хабарова О.С. Бурова С.В. Тураева Т.Л.	Методические указания к аудиторным занятиям и домашним заданиям по физике (Разноуровневые задачи по теме: «Электростатика») для студентов всех технических специальностей очной формы обучения	2010 магн. носитель	1
7.1.4 Программное обеспечение и интернет ресурсы				
7.1.4.1	InternetExplorer 6.0, Dreamweaver MX 2004, Dr. Web			
7.1.4.2	http://www.arnis.ru/gost_17799_common.htm			
7.1.4.3	**Мультимедийные лекционные демонстрации:**			
	– Технологии LAN – Структура современной корпоративной сети – Сети VPN – Удаленное управление компьютером			

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1	**Специализированная лекционная аудитория**, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой
8.2	**Дисплейный класс**, оснащенный компьютерными программами для проведения практических занятий
8.3	**Кабинеты**, оборудованные проекторами и интерактивными досками

ПРИЛОЖЕНИЕ 3

Карта обеспеченности рекомендуемой литературой

№ п/п	Авторы, составители	Заглавие	Год издания. Вид издания.	Обеспеченность
1. Основная литература				
Л1.1				
Л1.2				
2. Дополнительная литература				
Л2.1				
Л2.2				
3. Методические разработки				
Л3.1				
Л3.2				

Зав. кафедрой _____ / /

Директор НТБ _____ / /