Автономная некоммерческая образовательная организация высшего образования

Международный институт компьютерных технологий

Кафедра Информатики и вычислительной техники

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 027A948B004EB3AEBD434E04E7D63D214A
Владелец: РЫЖКОВ АЛЕКСАНДР ВЛАДИМИРОВИЧ
Действителен: с 04.09.2025 до 04.12.2026

УТВЕРЖДАЮ
Декан факультета высшего образования
_____ *Хорпяков О.С.*
«23» 01 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.27 «Защита информации»

Рекомендуется для направления подготовки (специальности) *54.03.01 «Дизайн»*

Профиль подготовки / специализации: *Дизайн программных интерфейсов и Web приложений*

Квалификация (степень) выпускника: бакалавр

Факультет высшего образования
Наименование факультета или факультетов

Воронеж
2026

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования № 1015, утвержденного Министерством образования РФ «13» августа 2020 г.
- учебного плана МИКТ по направлению/специальности 54.03.01 «Дизайн», одобренного Учёным советом вуза 23.01.2026, протокол №4.

Индекс- 54.03.01 Д

Рецензент: доцент кафедры «электропривод, автоматизация и управление в технических системах» Воронежского государственного технического университета, канд. техн. наук В.А. Трубецкой

Составитель (составители):
канд. техн. наук, доцент _____ А.В. Бобровников

Рабочая программа обсуждена на заседании кафедры «Информатики и вычислительной техники» « 10 » января 2026 г., протокол № 6

Рабочая программа одобрена методическим советом МИКТ
« 21 » января 2026 г., протокол № 4

1. Цель и задачи учебной дисциплины:

Целью преподавания дисциплины является формирование понятий о методах обеспечения информационной безопасности, методы обеспечения состояния информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокировки и т.п.

2. Место учебной дисциплины в структуре ОПОП:

Дисциплина Б1.О.27 относится к обязательным дисциплинам учебного плана специальности.

Для успешного освоения дисциплины необходимы знания, умения и навыки по следующим учебным курсам: высшая математика; физика, информатика.

Знания, приобретённые при изучении дисциплины «Защита информации» необходимы при освоении дисциплины «Безопасность компьютерных сетей».

3. Требования к результатам освоения дисциплины

В результате освоения дисциплины у обучаемого должны быть сформированы следующие компетенции:

- **УК-11.** Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности;
- **ОПК-6.** Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности;
- **ПК-2.** Способен понимать правовые аспекты работы с информацией и соблюдение требований законодательства в области защиты персональных данных и интеллектуальной собственности;
- **ПК-5**. Способен разрабатывать требования и проектировать графические программные интерфейсы, интерфейсы веб-приложений и интернет-сайтов, обеспечивающие удобство использования, высокую интерактивность и соответствие требованиям дизайна.

В результате изучения дисциплины студент должен:

Знать - задачи и функции защиты информации, архитектуру системы защиты информации, частные и обобщенные модели, а также классификацию методов решения задач защиты информации;

Уметь - определять степень защищенности информации.

Владеть - методами и средствами выявления угроз безопасности автоматизированным системам; навыками организации и обеспечения режима секретности; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации.

4. Объем дисциплины и виды учебной работы

Таблица 4.1

Распределение трудоемкости очной формы обучения	Объём	7-й семестр	Всего
1. Контактная работа по видам учебных занятий:			
Лекционные	часов	36	36
	З.Е.	1	1
Практические	часов	-	-
	З.Е.	-	-
Лабораторные работы	часов	36	36
	З.Е.	1	1
2. Самостоятельная работа	часов	72	72
	З.Е.	2	2
3. Зачет с оценкой	часов	+	+
Общая трудоемкость	часов	144	144
	З.Е.	4	4

Таблица 4.2

Распределение трудоемкости заочной формы обучения	Объём	10-й семестр	Всего
1	2		9
1. Контактная работа по видам учебных занятий:			
Лекционные	часов	12	12
	З.Е.	0,33	0,33
Лабораторные работы	часов	12	12
	З.Е.	0,33	0,33
2.Самостоятельная работа	часов	116	116
	З.Е.	3,23	3,23
3.Зачет с оценкой	часов	4	4
	З.Е.	0,11	0,11
Общая трудоемкость	часов	144	144
	З.Е.	4.0	4.0

5. Содержание дисциплины

Таблица 5.1

№ п/п	Наименование модуля (раздела) дисциплины	Содержание	Трудо-емкость	Компе-тенции
1	Введение в информационную безопасность компьютерных систем и сетей	Компьютерные системы и сети как объекты защиты информации. Каналы утечки информации и их классификация	48	УК-11 ОПК-6 ПК-2
2	Методы и средства защиты информации в ИКС	Модели систем защиты информации. Защита информации при построении компьютерных сетей. Защита информации при обработке на вычислительной технике.	48	ОПК-6 ПК-2
3	Методы и средства оценки параметров защищаемой информации	Методы оценки параметров защищаемой информации. Основные документы, регламентирующие требования по защите информации в ИКС	48	ОПК-6 ПК-5

6. Междисциплинарные связи с последующими дисциплинами

Таблица 6.1

№ п/п	**Наименование последующей дисциплины**	**Номера разделов данной дисциплины**		
		1	2	3
1	Безопасность компьютерных сетей	+	+	+

7. Распределение трудоемкости по видам занятий для очной формы обучения в часах

Таблица 7.1

№	Наименование модуля (раздела) дисциплины	Лекции	Лабораторные работы	Практические занятия	СРС	Всего
1	Введение в информационную безопасность систем и сетей связи	16	14	-	18	48
2	Методы и средства защиты информации в ИТКС	16	14	-	18	48
3	Методы и средства оценки параметров защищаемой информации	4	8	-	36	48
	Итого	36	36	-	72	144
	Итого по дисциплине:					144

8. Распределение трудоемкости по видам занятий для заочной формы обучения в часах

Таблица 8.1

№	Наименование модуля (раздела) дисциплины	Лекции	Лабораторные работы	СРС	Всего
1	Введение в информационную безопасность систем и сетей связи	4	4	36	44
2	Методы и средства защиты информации в ИТКС	4	4	36	44
3	Методы и средства оценки параметров защищаемой информации	4	4	44	52
	Итого	12	12	116	140
4	Контроль				4
	Итого по дисциплине:				144

9. Тематический план аудиторных занятий для дневной формы обучения

Таблица 9.1

	Вид занятия	Трудоемкость в часах	Формируемые компетенции
		всего .	
1 Введение в информационную безопасность			
1.1 Классификация угроз безопасности информации в информационно-коммуникационных системах	Лекция	4	УК-11 ОПК-6
1.2 Меры и средства защиты информации от угроз, связанных с НСД	Лекция	8	ОПК-6 ПК-2
1.3 Защита информации в системах обработки от случайных	Лаб. работа	4	ПК-5
1.4 Побочные излучения в информационно коммуникационных системах	Лаб. работа	4	ПК-5
1.5 Меры и средства защиты информации в ИКС от утечки по техническим каналам	Лекция	4	ПК-5
1.6 . Настройка системных параметров безопасности	Лаб. работа	6	ПК-5
2 Методы и средства защиты информации в ИКС			
2. Формальные модели обеспечения целостности данных и разграничения доступа в ИКС	Лекция	8	ОПК-6
2.2 Защита информации при построении сетей	Лаб. работа	4	ПК-5
2.3 Архивация и восстановление данных.	Лекция	4	ПК-5
2.4 Межсетевое экранирование и требования к межсетевым	Лаб. работа	4	ПК-5
2.5 Требования по защите информации, предъявляемые к средствам вычислительной тех-	Лекция	4	ПК-5
2.6 Обеспечение безопасности ресурсов с помощью разрешений файловой системы NTFS	Лаб. работа	6	ПК-5

3 Методы и средства оценки параметров защищаемой информации			
3.1 Методы оценки параметров защищаемой информации	Лекция	4	ОПК-6
3.2 Основные документы, регламентирующие требования по защите информации в ИКС	Лаб. работа	4	ПК-2
3.3 Общие вопросы обеспечения информационной безопас-	Лаб. работа	4	ПК-2

10 . Тематический план аудиторных занятий для заочной формы обучения

Таблица 10.1

	Вид занятия	Трудоемкость в часах	Формируемые компетенции
		всего	
1 Введение в информационную безопасность систем и сетей связи			
1.1 Классификация угроз безопасности информации в информационно-телекоммуникационных системах	Лекция	1	УК-11 ОПК-6
1.2 Меры и средства защиты информации от угроз, связанных с НСД	Лекция	1	ОПК-6 ПК-2
1.3 Защита информации в системах обработки от случайных	Лекция	1	ПК-5
1.4 Побочные излучения конструкций РЭС	Лаб. работа	2	ПК-5
1.5 Меры и средства защиты информации в ИТКС от утечки по техническим каналам	Лекция	1	ПК-5
1.6 Настройка системных параметров безопасности	Лаб. работа	2	ПК-5
2 Методы и средства защиты информации в ИТКС			
2.1 Формальные модели обеспечения целостности данных и разграничения доступа в ИТКС	Лекция	2	ОПК-6

2.2 Защита информации при построении сетей	Лаб. работа	2	ПК-5
2.3 Архивация и восстановление данных.	Лекция	2	ПК-5
2.4 Межсетевое экранирование и требования к межсетевым экранам	Лаб. работа	2	ПК-5
2.5 Требования по защите информации, предъявляемые к средствам вычислительной техники	Лекция	2	ПК-5
2.6 Обеспечение безопасности ресурсов с помощью разрешений файловой системы NTFS	Лаб. работа	2	ПК-5
3 Методы и средства оценки параметров защищаемой информации			
3.1 Методы оценки параметров защищаемой информации	Лекция	2	ОПК-6
3.2 Основные документы, регламентирующие требования по защите информации в ИТКС	Лаб. работа	1	ПК-2
3.3 Общие вопросы обеспечения информационной безопасности	Лаб. работа	1	ПК-2

11 Примерная тематика курсовых работ, проектов

При изучении дисциплины не предусмотрено выполнение курсовых работ и курсовых проектов.

12 Учебно-методическое и информационное обеспечение дисциплины

Перечень учебно-методического и информационного обеспечения учебной дисциплины представлен в Приложении 2.

13 Материально-техническое обеспечение дисциплины

Перечень материально-технического обеспечения учебной дисциплины представлен в Приложении 3.

14 Методические рекомендации по организации преподавания дисциплины

Дисциплина «Защита информации» опирается на понятия и методы, вводимые в ряде естественнонаучных и общетехнических дисциплин. Преподавание дисциплины должно строиться таким образом, чтобы все виды учебной работы были проникнуты системой междисциплинарных связей.

Изложение лекционного материала следует строго подчинять трем основным принципам: логической последовательности, взаимосвязанности, принципу - от простого к сложному. Основные аналитические соотношения должны быть получены доказательным путем на основе аргументированных математических моделей и ранее изложенных методов анализа, второстепенные выражения - достаточно обосновать физически. Изучение методов анализа после формулировки их сути и условий (ограничений) применения удобно проводить на конкретных объектах, в качестве которых следует выбрать основные классы колебаний и электрических цепей.

Студентам следует дать понять, что материал, изложенный в рамках лекционного курса, не является достаточным (как по объему, так и по степени конкретизации) для овладения дисциплиной, и поэтому крайне необходимым является самостоятельное изучение теоретического материала. В этой связи целесообразно ориентировать студентов на учебники и учебные пособия, имеющиеся в библиотеке института, а также снабдить студентов ссылками для доступа в Интернете к свободно распространяемым электронным версиям учебников и учебных пособий.

При организации аудиторных лабораторных занятий и самостоятельной работы студентов следует уделить значительное внимание решению учебных задач, иллюстрирующих, с одной стороны, основные положения теоретического материала и, с другой стороны, показывающих принципы использования общетеоретических положений для решения практических инженерных задач, что ведет к развитию навыков творческого мышления.

В целях более глубокого освоения дисциплины и стимулирования работы студента в течение всего учебного года целесообразно проводить текущий контроль уровня знаний и использовать рейтинговую оценку выявленных знаний.

Текущий контроль уровня знаний в рамках аудиторных занятий может осуществляться следующими способами:

1) посредством проведения письменных контрольных работ на решение типовых задач по текущим темам практических занятий;

2) проверкой результатов самостоятельных исследовательских работ, выполняемых студентами по желанию.

15. Воспитательная работа.
Духовно-нравственное воспитание

- развитие способности к сотрудничеству с окружающими в образовательной, общественно полезной, проектной и других видах деятельности.

Гражданско-правовое воспитание

- развитие студенческого самоуправления, совершенствование у обучающихся организаторских умений и навыков.

Профессиональное воспитание

- формирование творческого подхода к самосовершенствованию в контексте будущей профессии;
- повышение мотивации профессионального самосовершенствования обучающихся средствами изучаемых учебных дисциплин, практик, научно-исследовательской и других видов деятельности.

Приложения:

Приложение 1 - Фонд оценочных средств учебной дисциплины

Приложение 2 - Учебно-методическое и информационное обеспечение дисциплины

Приложение 3 - Материально-техническое обеспечение учебной дисциплины

Автономная некоммерческая образовательная организация высшего образования

Международный институт компьютерных технологий

Кафедра Информатики и вычислительной техники

УТВЕРЖДЕН

на заседании кафедры ИВТ

«_10_»__01_ 2025_г., протокол №_6_

Заведующий кафедрой

_____Слепокуров Ю.С.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Б1.О.27 «Защита информации»

Рекомендуется для направления подготовки (специальности) *54.03.01 «Дизайн»*

Профиль подготовки / специализации: *Дизайн программных интерфейсов и Web приложений*

Квалификация (степень) выпускника: бакалавр

Факультет высшего образования

Наименование факультета или факультетов

Составитель (составители):
канд. техн. наук, доцент _____ А.В. Бобровников

Экспертиза проведена доцентом кафедры «электропривод, автоматизация и управление в технических системах» Воронежского государственного технического университета, канд. Техн. Наук, В.А. Трубецким

Воронеж
2026

1. Модели формируемых компетенций

В процессе изучения дисциплины формируются следующие компетенции:

- УК-11. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности;
- ОПК-6. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности;
- ПК-2. Способен понимать правовые аспекты работы с информацией и соблюдение требований законодательства в области защиты персональных данных и интеллектуальной собственности;[ЮС1]
- ПК-5. Способен разрабатывать требования и проектировать графические программные интерфейсы, интерфейсы веб-приложений и интернет-сайтов, обеспечивающие удобство использования, высокую интерактивность и соответствие требованиям дизайна.

2. Требования к результатам освоения дисциплины:

В результате изучения дисциплины студент должен демонстрировать следующие результаты, характеризующие уровень сформированности компетенций:

УК-11.1 – знает основные особенности использования информации при противоправных действиях;

ОПК-6.1 - знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ПК-2.1 - умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ПК-5.1 - Имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

Указанные требования согласуются с требованиями профессионального стандарта от «18» ноября 2014 г. № 896н в части необходимых знаний и умений для выполнения следующих трудовых функций:

Наименование трудовой функции	Необходимо знать	Необходимо уметь	Результат обучения
Развертывание ИС у заказчика	Основы информационной безопасности организации	Выполнять параметрическую настройку ИС	УК- 11.1 ОПК- 6.1 ПК- 2.1 ПК-5.1
Разработка технологий интеграции ИС с существующими ИС заказчика	Основы информационной безопасности организации	Разрабатывать технологии обмена данными	ОПК- 6.1 ПК-5.1
Оптимизация работы ИС	Основы информационной безопасности организации	Разрабатывать метрики (количественные показатели) работы ИС	ОПК- 6.1 ПК- 2.1 ПК-5.1

3. Программа оценивания контролируемой компетенции

3.1 Текущая аттестация

Таблица 3.1

№	Контролируемый раздел (тема)	Код компетенции	Код результата	Наименование оценочного средства
1	2	3	4	5
1	Введение в информационную безопасность информационно-коммуникационных систем и сетей	УК - 11 ОПК - 6 ПК - 2 ПК -5	УК- 11.1 ОПК- 6.1 ПК- 2.1	Отчеты по лабораторным раб. №1-3
			ПК-5.1	РЗ №1
2	Методы и средства защиты информации в ИКС	ОПК-6	ОПК-6.1 ПК-5.1	Отчеты по лабораторным раб. № 4-6
			ПК-5.1	РЗ №2
3	Методы и средства оценки параметров защищаемой информации	ОПК-6	ОПК-6.1 ПК- 2.1	Отчеты по лабораторным раб. №7-8
			ПК- 2.1	РЗ №3

3.1.2 Примеры оценочных средств для текущего контроля

Учебный материал разделяется на содержательно-логически завершенные части (модули). Каждый модуль включает обязательные виды работ - лекционные и лабораторные занятия, самостоятельная работа.

Лабораторные работы и расчетные задания оцениваются в баллах, сумма которых дает рейтинг каждого учащегося. На основании полученного рейтинга выставляется зачет в конце семестра.

3.1.3 Критерии и шкалы оценивания

Тесты не используются и не оцениваются

3.1.4 Оценивание защиты лабораторных работ:

- 3 балла - правильно оформленный отчет и ответ на теоретические вопросы с существенными неточностями;

- 4 балла - правильно оформленный отчет и ответ на теоретические вопросы с несущественными неточностями;

- 5 баллов - правильно оформленный отчет и полный ответ на теоретические вопросы.

3.1.5 Оценивание расчётных заданий:

- 3 балла - расчётные формулы выбраны правильно, но имеются неточности, результат не соответствует контрольному значению;

- 4 балла - расчётные формулы выбраны правильно, результат не соответствует контрольному значению;

- 5 баллов - расчётные формулы выбраны правильно, результат соответствует контрольному значению.

3.2 Промежуточная аттестация

3.2.2 Вопросы для подготовки к промежуточной аттестации

1. Направления защиты информации в современных ИКС.
2. Состав средств подсистем, включаемых в подсистему защиты информации от несанкционированного доступа.
3. Состав средств и подсистем, включаемых в подсистему управления защитой информации.
4. Стадии создания систем защиты информации
5. Понятие угрозы информационной безопасности. Классификация угроз.
6. Общая технологическая схема выявления угроз информационной безопасности.
7. Угроза несанкционированного доступа.

8. Классификация атак в ИКС.
9. Внедрение в распределенную сеть ложного объекта путем навязывания ложного маршрута.
10. Внедрения в распределенную сеть ложного объекта на основе использования недостатков алгоритмов удаленного поиска.
11. Программно-математическое воздействие - основные направления НСД.
12. Классификация вредоносных программ и их принципы работы.
13. Способы реализации функций вредоносных программ.
14. Деструктивные функции вредоносных несетевых программ.
15. Угрозы вредоносных сетевых программ.
16. Классификация методов защиты от вредоносных программ.
17. Классификация мер и средств защиты информации от утечки по побочным электромагнитным излучениям и наводкам.
18. Метод экранирования технических средств.
19. Использование фильтрации информационных сигналов.
20. Метод пространственного и линейного зашумления.
21. Защита телефонных аппаратов и телефонных линий от утечки информации.
22. Способы защиты линий связи при передаче информации.
23. Криптография- основные понятия. Модель традиционного шифрования.
24. Типы криптосистем.
25. Типы криптоатак и стойкость алгоритмов.
26. Сети Фейстеля.
27. Структура шифра Фейстеля.
28. Стандарт шифрования данных DES
29. Криптосистемы шифрования данных RSA
30. Криптосистемы шифрования данных Эль-Гамаля.
31. Межсетевые экраны — назначение, классификация.
32. Классы защищенности межсетевых экранов.
33. Системная классификация моделей защиты информации.
34. Классификация методов статистического моделирования.
35. Обобщенная структура имитационной модели.
36. Классы защищенности ИТКС.
37. Методы оценки параметров защищаемой информации.
38. Структура и значения критериев оценки важности информации.
39. Критерии оценки адекватности информации.
40. Критерий релевантности информации.
41. Основные документы, регламентирующие требования по защите информации.
42. Специальные требования по защите конфиденциальной информации.

3.2.3 Форма билета для зачета

54.03.01 - Дизайн

Кафедра информатики и вычислительной техники
дисциплина - Защита информации

Билет №...

1. Формулировка вопроса для проверки уровня ЗНАТЬ
2. Формулировка вопроса для проверки уровня УМЕТЬ
3. Формулировка вопроса для проверки уровня ВЛАДЕТЬ

Преподаватель _____
Зав.кафедрой _____
_____ 202_ г.

3.2.3 Оценивание на промежуточной аттестации

Компоненты компетенции	Пороговый уровень (удовлетворительно или 3 балла)	Базовый (хорошо или 4 балла)	Повышенный (отлично или 5 баллов)
УК-11.1 ОПК-6.1	ответ на теоретические вопросы билета с существенными неточностями	ответ на теоретические вопросы билета с несущественными неточностями	полный ответ на теоретические вопросы билета и дополнительные вопросы
ПК-5.1	В расчётные формулы выбраны правильно, но имеются неточности, результат не соответствует контрольному значению	Расчётные формулы выбраны правильно, результат не соответствует контрольному значению.	Расчётные формулы выбраны правильно, результат соответствует контрольному значению
ПК2.1	Анализ исходных данных выполнен удовлетворительно, выбран неоптимальный путь решения, полученный результат не полностью удовлетворяет требованиям	Анализ условий выполнен правильно, выбран правильный путь решения, получено правильное решение поставленной задачи	Анализ условий выполнен правильно, выбран лучший путь решения, получено оптимальное решение поставленной задачи

Максимальное количество баллов, которое может получить обучаемый на промежуточной аттестации составляет 15, минимальное - 9.

Оценка отлично выставляется при сумме баллов от 14 до 15; (4+5+5; 5+5+5).

Оценка «хорошо» выставляется при сумме баллов от 12 до 13 (4+4+4; 3+4+5; 4+4+5).

Оценка «удовлетворительно» выставляется при сумме баллов от 9 до 11 (3+3+3; 3+3+4; 4+4+3; 3+3+5).

Приложение 2

Учебно-методическое и информационное обеспечение учебной дисциплины

1 Рекомендуемая литература

Основная литература:

1. Минаев В.А., Скрыль С.В., Фисун А.П., Потанин В.Е., Дворянкин С.В., Основы информационной безопасности: учебник.- Воронеж: ВИ МВД России.- 2001.
2. Нестеров С.А., Основы информационной безопасности : учебное пособие / Нестеров С.А.. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 c. — ISBN 978-5-7422-4331-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/43960.html (дата обращения: 25.03.2024)

Дополнительная литература:

3. Теоретические основы компьютерной безопасности: Учеб. пособие для вузов Девянин П.Н., Михальский О.О., Правиков Д.И.и др. / М.: Радио и связь, 2006.-192с.

2 Рекомендуемое программное обеспечение

Специальное программное обеспечение не предусмотрено.

3 Рекомендуемые базы данных, информационно-справочные и поисковые системы, периодика

http://sdo.iict.ru/course/view.php?id=367

Приложение 3

Материально-техническое обеспечение учебной дисциплины

1 В процессе преподавания дисциплины при проведении лекционных занятий используются презентации, выполненные в формате Microsoft Power Point и EXCEL, что вызывает необходимость использования компьютерных классов.

2 В процессе преподавания дисциплины для проведения лабораторных занятий, связанных с проведением расчетов необходимо использование компьютерных классов.