МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ЭМИТ

_____ Баркалов С.А._/

_____ 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационная безопасность»

Направление подготовки 09.03.03 Прикладная информатика

Профиль Проектирование информационно-аналитических систем высокотехнологичных производств

Квалификация выпускника бакалавр

Нормативный период обучения 4 года / 4 года 11 месяцев

Форма обучения очная / заочная

Год начала подготовки 2022

Автор программы _____ К.В.Славнов

Заведующий кафедрой
Базовая кафедра
кибернетики в системах
организационного
управления _____ В.Е.Белоусов

Руководитель ОПОП _____ В.Е.Белоусов

Воронеж 2022

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Целью дисциплины является изучение основных принципов, методов и средств защиты информации в процессе ее обработки, ознакомление студентов с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а так же с нормативными документами России по данному вопросу

1.2. Задачи освоения дисциплины

Получение студентами знаний по существующим угрозам безопасности информации, подбору и применению современных методов и способов защиты информации; формирование практических умений и навыков применения современных технологий обеспечения защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б.1 учебного плана.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Информационная безопасность» направлен на формирование следующих компетенций:

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

ПК-3 Способность осуществлять и обосновывать выбор проектных решений по видам обеспечения информационных систем

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-3	знать основные виды и классификацию угроз информационной безопасности
	уметь использовать безопасные методы работы в Интернете и с электронными почтовыми сервисами
	владеть навыками использования методов защиты информации различными способами
ОПК-4	знать классификацию угроз в зависимости от

	обрабатываемой информации, способа ее хранения и средств обработки
	уметь использовать нормативные документы в области защиты информации и в информационной безопасности
	владеть навыками применения методов аудита организации защиты информации на предприятии
ПК-3	Знать теоретико-методологические основы системного анализа; основные схемы и процессы имитационного моделирования
	Уметь использовать математические и инструментальные средства для решения задач управления, проводить исследовательскую работу по социально-экономической оценке и конкретных форм управления
	Владеть навыками разработки имитационной модели с использованием пакетов прикладных программ

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Информационная безопасность» составляет 5 зачетных единиц.

Распределение трудоемкости дисциплины по видам занятий

Очная форма обучения

Вид учебной работы	Всего часов	Семестр 7
Аудиторные занятия (всего)		
В том числе:		
Лекции		54
Практические занятия (ПЗ), в том числе в форме практической подготовки (*при наличии*)[1]		18
Лабораторные работы (ЛР), в том числе в форме практической подготовки (*при наличии*)		18
Самостоятельная работа		
Курсовой проект (работа) (есть, нет)		
Контрольная работа (есть, нет)		
Вид промежуточной аттестации (зачет, зачет с оценкой, экзамен)		
Общая трудоемкость час		180
зач. ед.		5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	Лаб. зан.	СРС	Всего, час
1	Тема 1. Теоретические основы информационной безопасности.	Современное состояние защиты информации. Понятие, основные определения и составляющие информационной безопасности. Доступность, целостность, конфиденциальность.					
		Кейсы по Основам информационной безопасности					
2	Тема 2. Актуальность защиты информации Важность и сложность проблемы информационной безопасности.	Анализ проблематики, связанной с информационной безопасностью. Проблемы защиты информации в интернете. Ценность информации.					
		Кейс по Актуальности защиты информации					

[1] Здесь и далее уточнение «в том числе в форме практической подготовки» пишется при наличии данного вида работ в учебном плане. Если дисциплина без практической подготовки, то данное уточнение надо удалить

3	Тема 3. Виды угроз. Наиболее распространенные угрозы, пути и каналы утечки информации, от кого они исходят и к чему приводят.	Изучение видов атак и методов взлома интрасетей злоумышленниками. Виды возможных нарушений информационной системы. Виды противников или «нарушителей».					
		Кейс по тематике видов угроз					
4	Тема 4. Вредоносное программное обеспечение.	Основные правила защиты от «компьютерных вирусов». Обзор и методика использования антивирусных программ. Восстановление пораженных «компьютерными вирусами» объектов					
		Кейс по вредоносным программным обеспечениям					
5	Тема 5. Основы законодательства в области информационной безопасности	Что такое законодательный уровень информационной безопасности и почему он важен. Обзор российского законодательства в области ИБ. Ответственность на нарушения ИБ.					
		Кейс по основам законодательства					
Итого							**180**

Практическая подготовка при освоении дисциплины (модуля) проводится путем непосредственного выполнения обучающимися отдельных элементов работ, связанных с будущей профессиональной деятельностью, способствующих формированию, закреплению и развитию практических навыков и компетенций по профилю соответствующей образовательной программы на практических занятиях и (или) лабораторных работах*:

№ п/п	Перечень выполняемых обучающимися отдельных элементов работ, связанных с будущей профессиональной деятельностью	Формируемые профессиональные компетенции
1	Программно-технические меры защиты информации в системах управления и автоматизации.	ОПК-3,ОПК-4, ПК-3
2	Основные понятия программно-технического уровня информационной безопасности.	ОПК-3,ОПК-4, ПК-3
3	Методы защиты информации в системах управления: ограничение доступа, разграничение доступа, разделение доступа, криптографическое преобразование информации, контроль и учет доступа, законодательные меры, обеспечение информационной безопасности в Internet.	ОПК-3,ОПК-4, ПК-3
4	Основные технологии построения защищенных ИС.	ОПК-3,ОПК-4, ПК-3
5	Технические средства защиты информации в системах управления.	ОПК-3,ОПК-4, ПК-3

5.2 Перечень лабораторных работ**

Что такое информационная безопасность?

2 Какие предпосылки и цели обеспечения информационной безопасности?

3 В чем заключаются национальные интересы РФ в информационной сфере?

4 Какие пути решения проблем информационной безопасности РФ существуют?

5 Каковы общие принципы обеспечения защиты информации?

6 Какие имеются виды угроз информационной безопасности предприятия (организации)?

7 Какие существуют источники наиболее распространенных угроз информационной безопасности?

8 Что включают в себя требования по обеспечению комплексной системы информационной безопасности?

9 Какие уровни информационной защиты существуют, их основные составляющие?

10 В чем заключаются задачи криптографии?

11 Какие системы шифрования вы знаете?

12 Что включает в себя защита информации от несанкционированного доступа?

13 В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?

14 Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?

15 Какие задачи выполняет подсистема управления доступом?

16 Какие требования предъявляются к подсистеме протоколирования аудита?

17 Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?

18 Какие функции выполняет служба регистрации и наблюдения?

19 Что такое информационно-опасные сигналы, их основные параметры?

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсового проекта (работы) в 7 семестре.

Примерная тематика курсового проекта (работы):

1 Какие имеются показатели защищенности межсетевых экранов?

2 Какая программа называется вирусом?

3 Какая атака называется атакой отказа в обслуживании?

4 Какие виды вирусов вы знаете?

5 Какие вирусы называются паразитическими?

6 Как распространяются вирусы?

7 Какие методы обнаружения вирусов вы знаете?

8 В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?

9 Какие существуют пути защиты информации в локальной сети?

10 Из каких этапов состоят работы по обеспечению информационной безопасности предприятия?

11 Что понимают под политикой информационной безопасности?

12 Что включает в себя политика информационной безопасности РФ?

13 Какие нормативные документы РФ определяют концепцию защиты информации?

14 В каком случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности?

15 Сформулируйте понятия «доступность», «целостность», «конфиденциальность информации»

16 Назовите наиболее распространенные пути и каналы утечки информации систем управления.

17 Сформулируйте достоинства и недостатки современных антивирусных программ.

18 Назовите мероприятия по защите информации от несанкционированного доступа.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-3	знать основные виды и классификацию угроз информационной безопасности	Полное или частичное посещение лекционных и практических занятий.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь использовать безопасные методы работы в Интернете и с электронными почтовыми сервисами	Полное или частичное посещение лекционных и практических занятий.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками использования методов защиты информации различными способами	Полное или частичное посещение лекционных и практических занятий.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-4	знать классификацию угроз в зависимости от обрабатываемой информации, способа ее хранения и средств обработки	Полное или частичное посещение лекционных и практических занятий.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь использовать нормативные документы в	Полное или частичное посещение лекционных и	Выполнение работ в срок,	Невыполнение работ в срок,

	области защиты информации и в информационной безопасности	практических занятий.	предусмотренный в рабочих программах	предусмотренный в рабочих программах
	владеть навыками применения методов аудита организации защиты информации на предприятии	Полное или частичное посещение лекционных и практических занятий.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-3	Знать теоретико-методологические основы системного анализа; основные схемы и процессы имитационного моделирования	Полное или частичное посещение лекционных и практических занятий.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь использовать математические и инструментальные средства для решения задач управления, проводить исследовательскую работу по социально-экономической оценке и конкретных форм управления	Полное или частичное посещение лекционных и практических занятий.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть навыками разработки имитационной модели с использованием пакетов прикладных программ	Решение прикладных задач в конкретной предметной области, выполнение плана работ по разработке курсового проекта	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в ___ семестре для очной формы обучения, в ___ семестре для очно-заочной (*при наличии*) формы обучения, в ___ семестре для заочной (*при наличии*) формы обучения по системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл	Неудовл
ОПК-3	знать основные виды и классификацию угроз информационной безопасности	Тест	Выполнение теста на 90-100%	Выполнение теста на 80- 90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	уметь использовать безопасные методы работы в Интернете и с электронными почтовыми сервисами	Решение стандартных практических	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

		задач		во всех задачах		
	владеть навыками использования методов защиты информации различными способами	Тест	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ОПК-4	знать классификацию угроз в зависимости от обрабатываемой информации, способа ее хранения и средств обработки	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь использовать нормативные документы в области защиты информации и в информационной безопасности	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками применения методов аудита организации защиты информации на предприятии	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-3	Знать теоретико-методологические основы системного анализа; основные схемы и процессы имитационного моделирования	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Уметь использовать математические и инструментальные средства для решения задач управления, проводить исследовательскую работу по социально-экономической оценке и конкретных форм управления	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть навыками разработки имитационной модели с использованием пакетов прикладных программ	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

Потенциальные угрозы, против которых направлены технические меры защиты информации:

а) потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей

б) потери информации из-за не достаточной установки сигнализации в помещении

в) потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения

Для защиты от злоумышленников необходимо использовать:

а) системное программное обеспечение

б) прикладное программное обеспечение

в) антивирусные программы

Что является наиболее надежным средством предотвращения потерь компьютерной информации при кратковременном отключении электроэнергии?

а) установка источников бесперебойного питания

б) такого средства не существует

в) перекидывать информацию на носитель, который не зависит от энергии

Программные средства защиты можно разделить на:

а) правовые, аппаратные, программные

б) административные меры защиты, включающие подготовку и обучение персонала, организацию тестирования и приема в эксплуатацию программ, контроль доступа в помещения и т.д.

в) криптография, антивирусные программы, системы разграничения полномочий, средства контроля доступа и т.д.

Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются:

а) вирусами

б) руткитами

в) червями

Уровень риска, который считается доступным для достижения желаемого результата, называется:

а) устойчивостью

б) терпимостью по отношению к риску

в) независимостью

Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется:

а) Троянской программой

б) червем

в) вирусом

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Документ, содержащий правила, общие принципы или характеристики, касающиеся различных видов деятельности или их результатов, …
    1. закон
    2. директивный документ
    3. план мероприятий
    4. нормативный документ

2. Рыночный жизненный цикл ПС дополнительно включает фазы:
    1. Торговый анализ.
    2. Фиксирование маркетинговой стратегии.
    3. Тестирование рынка.
    4. Коммерциализация.

3. Проверка соответствия формализованным правилам — это:
    1. Контроль полноты спецификаций.
    2. Верификация.
    3. Тестирование.
    4. Синтаксический контроль.

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Документ, содержащий правила, общие принципы или характеристики, касающиеся различных видов деятельности или их результатов, …
    1. закон
    2. директивный документ
    3. план мероприятий
    4. нормативный документ

2. Рыночный жизненный цикл ПС дополнительно включает фазы:
    1. Торговый анализ.
    2. Фиксирование маркетинговой стратегии.
    3. Тестирование рынка.
    4. Коммерциализация.

3. Проверка соответствия формализованным правилам — это:
    1. Контроль полноты спецификаций.
    2. Верификация.
    3. Тестирование.
    4. Синтаксический контроль.

7.2.4 Примерный перечень вопросов для подготовки к зачету**

Не предусмотрено учебным планом

7.2.5 Примерный перечень вопросов для подготовки к экзамену**

1. Что такое информационная безопасность?

2. Какие предпосылки и цели обеспечения информационной безопасности?

3. В чем заключаются национальные интересы РФ в информационной сфере?

4. Что включает в себя информационная борьба?

5. Какие пути решения проблем информационной безопасности РФ существуют?

6. Каковы общие принципы обеспечения защиты информации?

7. Какие имеются виды угроз информационной безопасности предприятия (организации)?

8. Какие источники наиболее распространенных угроз информационной безопасности существуют?

9. Какие виды сетевых атак имеются?

10.Какими способами снизить угрозу сниффинга пакетов?

11.Какие меры по устранению угрозы IP -спуфинга существуют?

12.Что включает борьба с атаками на уровне приложений?

7.2.6 Методика выставления оценки при проведении промежуточной аттестации

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Тема 1. Теоретические основы информационной безопасности.	ОПК-3,ОПК-4,ПК-3	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Тема 2. Актуальность защиты информации Важность и сложность проблемы информационной безопасности.	ОПК-3,ОПК-4,ПК-3	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
3	Тема 3. Виды угроз. Наиболее распространенные угрозы, пути и каналы утечки информации, от кого они исходят и к чему приводят.	ОПК-3,ОПК-4,ПК-3	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Тема 4. Вредоносное программное обеспечение.	ОПК-3,ОПК-4,ПК-3	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Тема 5. Основы законодательства в области информационной безопасности	ОПК-3,ОПК-4,ПК-3	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач

на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсового проекта осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.**

***текст приведен для примера*

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

1. Стандартизация, сертификация и управление качеством программного обеспечения: учеб. пособие / Т.Н. Ананьева, Н.Г. Новикова, Г.Н. Исаев. М.: ИНФРА-М, 2019. 232 с. (Высшее образование: Бакалавриат). www.dx.doi.org/10.12737/18657. - Режим доступа: http://znanium.com/catalog/product/1002357

2. Управление качеством программного обеспечения: Учебник / Б.В. Черников. - М.: ИД ФОРУМ: ИНФРА-М, 2012.- 240 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0499-2 - Режим доступа: http://znanium.com/catalog/product/256901.

3. Технология разработки программного обеспечения: Учеб. пос. / Л.Г. Гагарина, Е.В. Кокорева, Б.Д. Виснадул; Под ред. проф. Л.Г. Гагариной - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 400 с.: ил.; 60x90 1/16. - (Высшее обр.). (п) ISBN 978-5-8199-0342-1 - Режим доступа: http://znanium.com/catalog/product/389963.

4. Введение в архитектуру программного обеспечения: Учебное пособие / Гагарина Л.Г., Федоров А.Р., Федоров П.А. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 320 с.: 60x90 1/16. - (Высшее образование) (Переплёт 7БЦ) ISBN 978-5-8199-0649-1 - Режим доступа: http://znanium.com/catalog/product/542665.

5. Принципы и методы создания надежного программного обеспечения АСУТП: Методическое пособие / Мякишев Д.В. - Вологда: Инфра-Инженерия, 2017. - 114 с.: ISBN 978-5-9729-0179-1 - Режим доступа: http://znanium.com/catalog/product/943318.

6. Программные средства и механизмы разработки информационных систем: Учебное пособие / Лежебоков А.А. Таганрог: Южный федеральный университет, 2016. - 86 с.: ISBN 978-5-9275-2286-6 - Режим доступа: http://znanium.com/catalog/product/997088.

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем

1. Справочная правовая система КонсультантПлюс http://www.consultant.ru/

2. Межвузовская электронная библиотека (МЭБ) https://icdlib.nspu.ru/

3. Национальная электронная библиотека https://rusneb.ru/

4. Adobe Acrobat Reader. reader.html?promoid=81G55Y1C&mv=other). (https://acrobat.adobe.com/us/en/acrobat/pdf2.

5. Бесплатная интегрированная среда разработки Anaconda.

6. Система электронного обучения https://elearning.utmn.ru

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Компьютерный класс 2303 в составе:

- Рабочие станции –10 комплектов;
- Принтер лазерный -1 комплект;
- Комплект сетевого оборудования для организации ЛВС и доступа к ресурсам сети ВГТУ (в том числе к нейрокомпьютеру);
- Мультимедиапроектор и экран;
- Программы: Google Colab, PyCharm, postgreSQL.

Автоматизированные обучающие системы для изучения прикладных программных продуктов, тестирующий комплекс контроля качества обучения, интегрированная система мониторинга хода учебного процесса кафедры.

10 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Информационная безопасность» читаются лекции, проводятся практические занятия, выполняется курсовой проект.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических навыков расчета инженерных систем теплогазоснабжения, подбора основного и вспомогательного оборудования. Занятия проводятся путем решения конкретных задач в аудитории.

Большое значение по закреплению и совершенствованию знаний имеет самостоятельная работа студентов. Информацию о всех видах самостоятельной работы студенты получают на занятиях.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта. Освоение дисциплины оценивается на экзамене.

Вид учебных занятий	Деятельность студента (*особенности деятельности студента инвалида и лица с ОВЗ, при наличии таких обучающихся*)
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практические занятия	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Подготовка к экзамену	При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и решение задач на практических занятиях.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП