

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Горбунов Алексей Александрович
Должность: Заместитель ректора университета по научной работе
Дата подписания: 23.07.2025 14:10:40
Уникальный программный ключ:
286e49ee1471d400cc1f45539d51ed7bbf0e9cc7

ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ
ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ**

**Специалитет по специальности
10.05.03 – Информационная безопасность автоматизированных систем**

Специализация «Анализ безопасности информационных систем»

Санкт-Петербург

1. Цели и задачи дисциплины

Цель освоения дисциплины:

– формирование к обучающимся компетенций, необходимых специалистам, для обеспечения безопасности значимых объектов критической инфраструктуры.

Перечень компетенций, формируемых в процессе изучения дисциплины

Компетенции	Содержание
ПК - 4	Способен формировать требования к защите информации в автоматизированных системах, используемых в том числе на объектах критической информационной инфраструктуры

Задачи дисциплины:

- выделение объектов, угроз, определение способов и средств защиты объектов критической инфраструктуры;
- освоение на практике специфики проведения комплекса мероприятий по определению оснований для отнесения организации к объектам критической информационной инфраструктуры;
- изучение особенностей проведения инвентаризации и категорирования объектов критической информационной инфраструктуры.

2. Перечень планируемых результатов обучения дисциплины, соотнесенных с планируемыми результатами освоения образовательной программы

Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ПК-4.1. Руководствуется требованиями нормативных правовых актов в области защиты информации значимых объектов критической информационной инфраструктуры; основами построения и функционирования современных и перспективных автоматизированных систем управления МЧС России; методикой формирования моделей нарушителей и методику оценки угроз безопасности информации значимых объектов критической информационной инфраструктуры; методы и средства обеспечения безопасности значимых объектов критической информационной инфраструктуры	Знает содержание и порядок деятельности персонала по эксплуатации систем информационной безопасности объектов критической информационной инфраструктуры, общие принципы организации защиты объектов критической информационной инфраструктуры и ее частей Умеет разрабатывать организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры,
ПК-4.2. Проводит анализ исходных данных и проектных решений при разработке подсистем и средств обеспечения безопасности значимых объектов	Знает нормативную базу, регламентирующую процессы проектирования, построения и эксплуатации систем информационной безопасности объектов критической

критической информационной инфраструктуры; использует комплексы технических средств автоматизации управления подразделении МЧС России; определяет источники угроз безопасности информации и проводит оценку возможностей нарушителей по реализации угроз безопасности информации; планирует и разрабатывает организационно-правовые и программно-технические меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры	информационной инфраструктуры, общие принципы проектирования систем информационной безопасности объектов критической информационной инфраструктуры и ее частей, Умеет применять на практике знания, полученные при изучении комплексов средств автоматизации управления, информирования и оповещения элементов РСЧС и населения
ПК-4.3. Демонстрирует навыки проектирования подсистем безопасности значимых объектов критической информационной инфраструктуры; использования комплексов технических средств автоматизации деятельности подразделений МЧС России	Знает принципы построения систем информационной безопасности объектов критической информационной инфраструктуры и ее частей, состав технико-экономического обоснования проектируемых систем информационной безопасности объектов критической информационной инфраструктуры и ее частей Умеет применять технические меры обеспечения безопасности значимых объектов критической информационной инфраструктуры, организовывать защиту объектов критической информационной инфраструктуры и ее частей с учетом действующих нормативных и методических документов

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Обеспечение безопасности критической информационной инфраструктуры» относится к части, формируемой участниками образовательных отношений, образовательной программы специалитета по специальности **10.05.03 – Информационная безопасность автоматизированных систем**, специализация – **Анализ безопасности информационных систем**.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачётных единиц, 180 часов.

4.1 Распределение трудоемкости дисциплины по видам работ по семестрам для очной формы обучения

Вид учебной работы	Трудоемкость			
	з.е.	час.	по семестрам	
			10	11
Общая трудоемкость дисциплины по учебному плану	5	180	72	144
Контактная работа		74	36	38
Лекции		28	14	14
Практические занятия		44	22	22
Консультация		2		2
Самостоятельная работа		70	36	34
Зачет с оценкой			+	
Экзамен		36		+

4.2. Тематический план, структурированный по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий для очной формы обучения

Наименование разделов	Всего часов	Количество часов по видам занятий					Самостоятельная работа
		Лекции	Практические занятия	Лабораторные работы	Консультации	Контроль	
10семестр							
Раздел 1. Понятие критической информационной инфраструктуры	24	6	6				12
Раздел 2. Правовое обеспечение критической информационной инфраструктуры	24	4	8				12
Раздел 3. Категории объектов критической информационной инфраструктуры	24	4	8				12
Зачет с оценкой						+	
Итого за 10 семестр	72	14	22				36
11 семестр							
Раздел 4. Технические и организационные меры безопасности значимых объектов	26	6	8				12
Раздел 5. Модели угроз и выбор мер защиты объектовкритической информационной инфраструктуры	24	4	8				12
Раздел 6. Организационно-распорядительные документы по обеспечению безопасностизначимых объектов критической информационной инфраструктуры	20	4	6				10
Консультация	2				2		
Экзамен	36					+	

Итого за 11 семестр	108	14	22		2	36	34
Всего за 10, 11 семестр	180	28	44		2	36	88

4.3 Содержание дисциплины для очной формы обучения

Раздел 1. Понятие критической информационной инфраструктуры

Лекции. Термины и определения, понятие критической информационной инфраструктуры (КИИ), объекты КИИ.

Практические занятия. Термины и определения, понятие критической информационной инфраструктуры (КИИ), объекты КИИ.

Самостоятельная работа. Самостоятельно е изучение рекомендуемых источников и материалов.

Рекомендуемая литература:

Основная литература: [1,2];

Дополнительная литература: [1].

Раздел 2. Правовое обеспечение критической информационной инфраструктуры

Лекции. Документы, определяющие регулирование отношений в области обеспечения безопасности КИИ. Оценка безопасности КИИ. Государственный контроль в области обеспечения безопасности значимых объектов КИИ.

Практические занятия. Документы, определяющие регулирование отношений в области обеспечения безопасности КИИ. Оценка безопасности КИИ. Государственный контроль в области обеспечения безопасности значимых объектов КИИ. Постановление от 8 февраля 2018 года №127. О порядке категорирования объектов критической информационной инфраструктуры. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Самостоятельная работа. Самостоятельно е изучение рекомендуемых источников и материалов.

Рекомендуемая литература:

Основная литература: [1,2];

Дополнительная литература: [1].

Раздел 3. Категории объектов критической информационной инфраструктуры

Лекции. Классификация АСУТП. Критерии значимости объектов КИИ РФ и их значения. Сведения об объекте КИИ и угрозах ИБ. Нарушители ИБ объектов КИИ. Организационные и технические меры, применяемые для обеспечения ИБ КИИ.

Практические занятия. Классификация АСУТП по сфере функционирования, по виду системы, по Приказу ФСТЭК России

№31. Критерии значимости объектов КИИ РФ и их значения. Сведения об объекте КИИ и угрозах ИБ. Нарушители ИБ объектов КИИ. Организационные и технические меры, применяемые для обеспечения ИБ КИИ.

Самостоятельная работа. Анализ возможных источников угроз и действий предполагаемых нарушителей. Угрозы безопасности информации объекта КИИ. Построение модели угроз и нарушителей объектов КИИ. Процедуры выявления и анализа угроз безопасности информации, обрабатываемой объектом КИИ. Оценка масштаба последствий и соотнесение со значениями показателей категорий. Определение категории значимости объекта КИИ. Оформление и передача в ФСТЭК России результатов категорирования. Внесение изменений в результаты категорирования. Подготовка отчетных документов и контроль результатов категорирования объектов КИИ.

Рекомендуемая литература:

Основная литература: [1,2];

Дополнительная литература: [1].

Раздел 4. Технические и организационные меры безопасности значимых объектов

Лекции. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Анализ угроз и разработка модели угроз. Проектирование системы безопасности значимого объекта КИИ. Разработка рабочей и эксплуатационной документации.

Практические занятия. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Анализ угроз и разработка модели угроз. Проектирование системы безопасности значимого объекта КИИ. Разработка рабочей и эксплуатационной документации. Приказ № 235 от 21.12.2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

Самостоятельная работа. Система безопасности значимого объекта КИИ. Порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Стадии (этапы) работ по созданию систем безопасности объекта КИИ. Требования к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования. Разработка организационно-распорядительных документов по безопасности значимых объектов КИИ.

Рекомендуемая литература:

Основная литература: [1,2];

Дополнительная литература: [1].

Раздел 5. Модели угроз и выбор мер защиты объектов критической информационной инфраструктуры

Лекции. Классификация уязвимостей информационной системы, причины возникновения угроз безопасности. Формирование технического задания на создание или модификацию системы защиты объекта критической информационной инфраструктуры. Обсуждение правил выбора средств защиты информации для реализации организационных и технических мер.

Практические занятия. Классификация уязвимостей информационной системы, причины возникновения угроз безопасности. Формирование технического задания на создание или модификацию системы защиты объекта критической информационной инфраструктуры. Обсуждение правил выбора средств защиты информации для реализации организационных и технических мер.

Самостоятельная работа. Модели правового регулирования в сфере обеспечения безопасности КИИ. Невластные субъекты обеспечения безопасности КИИ, их правовой статус. Публичные органы в сфере обеспечения безопасности КИИ, их полномочия, взаимодействие между собой и с субъектами. Сравнительно-правовой анализ предлагаемых экономических моделей распределения издержек по обеспечению безопасности КИИ.

Рекомендуемая литература:

Основная литература: [1,2];

Дополнительная литература: [1].

Раздел 6. Организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры

Лекции. Организационно-распорядительные документы по безопасности значимых объектов, определяющие порядок и правила обеспечения безопасности значимых объектов КИИ, определяющие порядок и правила функционирования системы безопасности значимых объектов КИИ.

Практические занятия. Организационно-распорядительные документы по безопасности значимых объектов, определяющие порядок и правила обеспечения безопасности значимых объектов КИИ, определяющие порядок и правила функционирования системы безопасности значимых объектов КИИ.

Самостоятельная работа. Правила осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ. Правила организации повышения квалификации специалистов по ЗИ и должностных лиц, ответственных за организацию ЗИ в ОГВ, ОМС, организациях с госучастием и организациях ОПК. Порядок ведения реестра значимых объектов КИИ РФ. Итоги проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ. Порядок обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств,

международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядок получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения. Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ.

Рекомендуемая литература:

Основная литература: [1,2];

Дополнительная литература: [1].

5. Методические рекомендации по организации изучения дисциплины

При реализации программы учебной дисциплины используется традиционная образовательная технология, основой которой является системный принцип построения разделов и тем, используются лекционные, практические занятия и лабораторная работа.

Общими целями занятий являются:

- обобщение, систематизация, углубление, закрепление теоретических знаний по конкретным темам дисциплины;
- формирование умений применять полученные знания на практике, реализация единства интеллектуальной и практической деятельности;
- выработка при решении поставленных задач профессионально значимых качеств: самостоятельности, ответственности, точности, творческой инициативы.

Целями лекции являются:

- дать систематизированные научные знания по дисциплине, акцентировав внимание на наиболее сложных вопросах;
- стимулировать активную познавательную деятельность обучающихся, способствовать формированию их творческого мышления.

В ходе практического занятия обеспечивается процесс активного взаимодействия обучающихся с преподавателем; приобретаются практические навыки и умения. Цель практического занятия: углубить и закрепить знания, полученные на лекции, формирование навыков использования знаний для решения практических задач; выполнение тестовых заданий по проверке полученных знаний и умений.

Самостоятельная работа обучающихся направлена на углубление и закрепление знаний, полученных на лекциях и других занятиях, выработку навыков самостоятельного активного приобретения новых, дополнительных знаний, подготовку к предстоящим занятиям.

6. Оценочные материалы по дисциплине

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины, проводится в соответствии с содержанием дисциплины по видам занятий в форме типовых контрольных заданий.

Промежуточная аттестация обеспечивает оценивание промежуточных и окончательных результатов освоения дисциплины, проводится в форме зачета в 10 семестре и экзамена в 11 семестре.

6.1. Примерные оценочные материалы:

6.1.1. Текущего контроля

Примерные вопросы для теста:

1. Какое из определений информационных технологий верно
 - a) процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
 - b) приёмы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных;
 - c) ресурсы, необходимые для сбора, обработки, хранения и распространения информации;
 - d) все перечисленное.
2. Безопасность информации
 - a) состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность;
 - b) состояние, при котором невозможно изменить информацию;
 - c) состояние, обеспечивающее целостность и защищенность информации;
 - d) состояние, при котором злоумышленник не может получить информацию.
3. Безопасность критической информационной инфраструктуры
 - a) состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;
 - b) состояние защищенности, при котором обеспечены конфиденциальность, доступности и целостность информации;
 - c) состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование;
 - d) состояние, обеспечивающее целостность и защищенность информации.
4. Доступ к информации

- a) возможность получения информации и ее использования;
 - b) состояние доступности;
 - c) возможность проводить сбор, обработку и передачу информации
 - d) возможность изменения информации
5. Значимый объект критической информационно-инфраструктуры
- a) объект критической информационно-инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационно-инфраструктуры;
 - b) объект критической информационно-инфраструктуры, которому присвоена одна из категорий значимости;
 - c) информационно-телекоммуникационная сеть;
 - d) автоматизированная система управления субъекта критической информационно-инфраструктуры.
6. Объект критической информационно-инфраструктуры
- a) информационная система, информационно-телекоммуникационная сеть, автоматизированная система управления субъекта критической информационно-инфраструктуры;
 - b) автоматизированная система управления субъекта критической информационно-инфраструктуры;
 - c) объект критической информационно-инфраструктуры, которому присвоена одна из категорий значимости;
 - d) который включен в реестр значимых объектов критической информационно-инфраструктуры.
7. Субъекты критической информационно-инфраструктуры
- a) государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы;
 - b) информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно- энергетического комплекса, в области атомной энергии, оборонной, ракетно- космической, горнодобывающей, металлургической и химической промышленности,
 - c) российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей;
 - d) все выше перечисленное.
8. Какой закон регулирует отношения в области обеспечения безопасности КИИ РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

- a) Федеральный закон от 26.07.2017 № 187ФЗ;
 - b) Приказ ФСБ России от 19.06.2019 № 281;
 - c) Приказ ФСТЭК России от 25 декабря 2017 г. № 239;
 - d) Постановление Правительства РФ от 8 февраля 2018 г. № 127.
9. Компьютерный инцидент
- a) любое реальное или предполагаемое событие имеющее отношение к безопасности компьютерной системы или компьютерной сети;
 - b) атака на компьютерную систему;
 - c) изменение системы безопасности компьютерной сети;
 - d) событие изменяющее компьютерную систему.
10. Под ... понимается установление соответствия объекта КИИ критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.
- a) категорированием;
 - b) идентификацией;
 - c) установлением значимости;
 - d) обеспечением безопасности.

Примерные вопросы для опроса:

- 1. Классификация АСУТП: требования, параметры, сроки.
- Категорирование объектов критической информационной инфраструктуры
- 2. Разработка модели угроз
 - 3. Выбор мер защиты объектов информатизации
 - 4. Сетевые средства ИнфоТеКС для защиты АСУ КИИ
 - 5. Средства VipNet Coordinator IG

6.1.2. Промежуточной аттестации

Примерный перечень вопросов, выносимых на зачет

1. Состав технических мер по защите КИИ согласно приказу №239 ФСТЭК
2. Основные законы в сфере безопасности КИИ
3. Перечислите потенциальные сферы объектов КИИ, кратко охарактеризуйте их
4. Как определяются категории значимости объектов КИИ
5. Основные регуляторы объектов КИИ, их функции
6. Какая информация включается в реестр КИИ
7. Основные требования и последовательность реализаций требований к ИБ объекта КИИ
8. Классификация угроз безопасности объектов КИИ
9. Состав системы безопасности значимых объектов
10. Требования к средствам системы безопасности объектов КИИ

Примерный перечень вопросов, выносимых на экзамен

1. Правовые основы понятия критической информационной инфраструктуры.
2. Критическая информационная инфраструктура как объект обеспечения безопасности.
3. Анализ существующих методов обеспечения информационной безопасности критической информационной инфраструктуры.
4. Принципы обеспечения комплексной безопасности критической информационной инфраструктуры.
5. Изучение деятельности и организационной структуры организации КИИ.
6. Анализ технической архитектуры организации КИИ.
7. Анализ программной архитектуры и данных, обрабатываемых организацией КИИ.
8. Анализ обрабатываемых в организации данных КИИ.
9. Выявление критических процессов и определение объектов критической информационной инфраструктуры организации
10. Оценка факторов активности потенциального злоумышленника в контексте информационной безопасности организации.
11. Анализ уязвимостей и угроз безопасности организации.
12. Разработка модели актуальных угроз безопасности объектов критической инфраструктуры организации.
13. Определение категории выявленных объектов критической информационной инфраструктуры организации.
14. Определение оптимального комплекса организационных мер и методов обеспечения информационной безопасности.
15. Определение оптимального комплекса программно-аппаратных мер и методов обеспечения информационной безопасности в части технической и физической защиты.

16. Разработка мер защиты информации в целях нейтрализации выявленных актуальных угроз.

6.2. Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок

Система оценивания включает:

Форма контроля	Показатели оценивания	Критерии выставления оценок	Шкала оценивания
зачет	правильность и полнота ответа	дан правильный, полный ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; могут быть допущены недочеты, исправленные самостоятельно в процессе ответа; дан правильный, недостаточно полный ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи; могут быть допущены недочеты, исправленные с помощью преподавателя; дан недостаточно правильный и полный ответ; логика и последовательность изложения имеют нарушения; в ответе отсутствуют выводы.	зачтено
		ответ представляет собой разрозненные знания с существенными ошибками по вопросу; присутствуют фрагментарность, нелогичность изложения; дополнительные и уточняющие вопросы не приводят к коррекции ответа на вопрос.	не зачтено
экзамен	правильность и полнота ответа	дан правильный, полный ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; могут быть допущены недочеты, исправленные самостоятельно в процессе ответа.	отлично
		дан правильный, недостаточно полный ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи; могут быть допущены недочеты, исправленные с помощью	хорошо

		преподавателя.	
		дан недостаточно правильный и полный ответ; логика и последовательность изложения имеют нарушения; в ответе отсутствуют выводы.	удовлетворительно
		ответ представляет собой разрозненные знания с существенными ошибками по вопросу; присутствуют фрагментарность, нелогичность изложения; дополнительные и уточняющие вопросы не приводят к коррекции ответа на вопрос.	неудовлетворительно

7. Ресурсное обеспечение дисциплины.

7.1. Лицензионное и свободно распространяемое программное обеспечение

Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

1. Лицензия №217800111-ore-2.12-client-6196

Выдана «ФГБОУ ВО Санкт-Петербургский университет ГПС МЧС России» на право использования: Astra Linux Common Edition релиз Орел

Срок действия: бессрочно

2. Лицензия №217800111-alse-1.7-client-medium-x86_64-0-14545

Выдана «ФГБОУ ВО Санкт-Петербургский университет ГПС МЧС России» на право использования: Astra Linux Special Edition

Срок действия: бессрочно

3. Лицензия №217800111-alse-1.7-client-medium-x86_64-0-14544

Выдана «ФГБОУ ВО Санкт-Петербургский университет ГПС МЧС России» на право использования Astra Linux Special Edition

Срок действия: бессрочно

4. ПО «Р7-Офис. Профессиональный»

Выдана: «ФГБОУ ВО Санкт-Петербургский университет МЧС России»

Срок действия: бессрочно

7.2. Профессиональные базы данных и информационные справочные системы

1. Сервер органов государственной власти Российской Федерации <http://россия.пф/> (свободный доступ);

2. Портал открытых данных Российской Федерации <https://data.gov.ru/> (свободный доступ);

3. Федеральный портал «Российское образование» <http://www.edu.ru> (свободный доступ);

4. Система официального опубликования правовых актов в электронном виде <http://publication.pravo.gov.ru> (свободный доступ);

5. Федеральный портал «Совершенствование государственного управления» <https://ar.gov.ru> (свободный доступ);
6. Электронная библиотека университета <http://elib.igps.ru> (авторизованный доступ);
7. Электронно-библиотечная система «ЭБС IPR BOOKS» <http://www.iprbookshop.ru> (авторизованный доступ).
8. Электронно-библиотечная система "Лань" <https://e.lanbook.com> (авторизованный доступ).

7.3. Литература

Основная литература:

1. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — 2-е изд. — Саратов : Вузовское образование, 2024. — 214 с. — ISBN 978-5-4487-1026-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/142805.html>
2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 3-е изд. — Саратов : Профобразование, 2024. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/145912.html>

Дополнительная литература:

1. Газизов, А. Р. Организационное и правовое обеспечение информационной безопасности : учебное пособие / А. Р. Газизов ; под редакцией А. Р. Айдиняна. — Ростов-на-Дону : Донской государственный технический университет, 2017. — 156 с. — ISBN 978-5-7890-1384-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/117813.html> (дата обращения: 28.02.2025). — Режим доступа: для авторизир. пользователей. — DOI: <https://doi.org/10.23682/117813>

7.4. Материально-техническое обеспечение

Для проведения и обеспечения занятий используются помещения, которые представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения: автоматизированное рабочее место преподавателя, маркерная доска, мультимедийный проектор, документ-камера, посадочные места обучающихся.

Помещения для практических занятий и самостоятельной работы обучающихся оснащены компьютерной техникой, с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде университета.

Автор: кандидат технических наук, доцент Матвеев Александр Владимирович.