ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ 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 обучающихся 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 по дисциплине, соотнесенных с индикаторами достижения компетенций

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** нормативнуюбазу, 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 ОПОП

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

Дисциплина «Обеспечение безопасности критической информационной инфраструктуры» реализуется:

Для очной формы обучения в рамках обязательной части образовательной программы в объеме 180 академических часов (5 зачетных единиц).

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, в том числе:		**74**	**36**	**38**
Аудиторные занятия		**74**	**36**	**36**
Лекции (Л)		28	14	14
Практические занятия (ПЗ)		44	22	22
Консультация		2		2
Самостоятельная работа (СРС)		**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 и тем	**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	20	4	6				10

объектов критической информационной инфраструктуры							
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

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 [1,2];

дополнительная [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 [1,2];

дополнительная [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 по- следствий и соотнесение со значениями показателей категорий. Определение категории значимости объекта КИИ. Оформление и передача в ФСТЭК России результатов категорирования. Внесение изме- нений в результаты категорирования. Подготовка отчетных документов и контроль результатов кате- горирования объектов КИИ.

Рекомендуемая литература:

основная [1,2];

дополнительная [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 [1,2];

дополнительная [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 [1,2];

дополнительная [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 [1,2];

дополнительная [1].

5. Методические рекомендации по организации изучения дисциплины «Обеспечение безопасности критической информационной инфраструктуры»

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

На всех лекционных занятиях, целью которых является приобретение знаний, используется мультимедийный проектор с комплектом презентаций.

Общими дидактическими целями практического занятия являются:

- обобщение, систематизация, углубление, закрепление теоретических знаний по конкретным темам учебной дисциплины;
- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;
- выработка при решении поставленных задач профессионально значимых качеств: самостоятельность, ответственность, точность, творческая инициатива.

Активно используется самостоятельное выполнение каждым обучающимся учебной группы в течение 2 часов (после изучения теоретического материала каждой темы учебной дисциплины и проведения по ней ряда аудиторных практических занятий) индивидуальных практических заданий по изученной теме. Занятия проводятся в процессе активного взаимодействия с преподавателями.

Цель решения индивидуальных практических заданий - проверка уровня индивидуальной готовности обучающегося к решению практических задач по должностному предназначению на основе материала изученной темы.

Образовательными задачами индивидуальных заданий являются:

- глубокое изучение лекционного материала, изучение методов работы с учебной литературой, получение персональных консультаций у преподавателя;
- решение спектра практических задач, в том числе профессиональных (анализ производственных ситуаций, решение ситуационных задач, и т.п.);
- выполнение вычислений, расчетов;
- работа с нормативными документами, инструктивными материалами, справочниками.

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 «Обеспечение безопасности критической информационной инфраструктуры»

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 с оценкой 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, доступностьи 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 информационной инфраструктуры

a) объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

b) объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости;

c) информационно-телекоммуникационная сеть;

d) автоматизированная система управления субъекта критической информационной инфраструктуры.

6. Объект критической информационной инфраструктуры

a) информационная система, информационно-телекоммуникационная сеть, автоматизированная система управления субъекта критической информационнойинфраструктуры;

b) автоматизированная система управления субъекта критической информационной инфраструктуры;

c) объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости;

d) который включен в реестр значимых объектов критической информационной инфраструктуры.

7. Субъекты критической информационной 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 безопасностикомпьютерной 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 объектовкритической 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 с оценкой
10 семестр

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

Примерный перечень вопросов, выносимых на экзамен
11 семестр

1. Правовые основы понятия критической информационной инфраструктуры.
2. Критическая информационная инфраструктура как объект обеспечения безопасности.
3. Анализ существующих методов обеспечения информационной безопасности критическойинформационной инфраструктуры.
4. Принципы обеспечения комплексной безопасности критической информационнойинфраструктуры.
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

Форма контроля	Показатели оценивания	Критерии выставления оценок	Шкала оценивания
зачёт с оценкой (экзамен)	правильность и полнота ответа; выполнение контрольных нормативов	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; выполнение контрольных нормативов более половины на оценку «отлично», остальные не ниже «хорошо».	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 преподавателя; выполнение контрольных нормативов более половины на оценку «хорошо»,	Хорошо

		остальные не ниже «удовлетворительно».	
		дан недостаточно правильный и полный ответ, логика и последовательность изложения имеют нарушения, в ответе отсутствуют выводы; выполнение контрольных нормативов более половины на оценку «удовлетворительно», остальные не ниже «отлично» и «хорошо» или все «удовлетворительно».	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; выполнение одного и более контрольного норматива на оценку «неудовлетворительно».	Неудовлетворительно

7. Ресурсное обеспечение дисциплины «Обеспечение безопасности критической информационной инфраструктуры»

7.1. Лицензионное и свободно распространяемое программное обеспечение

Перечень лицензионного и свободно распространяемого программного обеспечения:

- МойОфис Образование [ПО-41В-124] - Полный комплект редакторов текстовых документов и электронных таблиц, а также инструментарий для работы с графическими презентациями [Свободно распространяемое. Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 4557]

- Astra Linux Common Edition релиз Орел [ПО-25В-603] - Операционная система общего назначения "Astra Linux Common Edition" [Коммерческая (Full Package Product). Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 4433]

7.2. Профессиональные базы данных и информационные справочные системы

1. Информационная система «Единое окно доступа к образовательным ресурсам» [Электронный ресурс]. – Режим доступа: http://window.edu.ru/, доступ только после самостоятельной регистрации

2. Научная электронная библиотека «eLIBRARY.RU» [Электронный ресурс]. – Режим доступа: https://www.elibrary.ru/, доступ только после самостоятельной регистрации

3. Справочная правовая система «КонсультантПлюс: Студент» [Электронный ресурс]. – Режим доступа: http://student.consultant.ru/, свободный доступ

4. Информационно-правовой портал «Гарант» [Электронный ресурс]. – Режим доступа: http://www.garant.ru/, свободный доступ

7.3. Литература

Основная литература:

1. Организационно-правовое обеспечение информационной безопасности : учебник / А.А. Стрельцов [и др.].. — Москва : Московский государственный технический университет имени Н.Э. Баумана, 2018. — 292 с. — ISBN 978-5-7038-4723-7. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/110777.html (дата обращения: 30.08.2023). — Режим доступа: для авторизир. пользователей
2. Бельская, Н. М. Организационное и правовое обеспечение информационной безопасности : методические указания / Н. М. Бельская, Н. И. Козырева, И. С. Макаров. — Самара : ПГУТИ, 2021. — 31 с. — Текст : электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/301040 (дата обращения: 30.08.2023). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

1. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности : учебное пособие / Г. П. Жигулин. — Санкт-Петербург : НИУ ИТМО, 2014. — 173 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/70952 (дата обращения: 30.08.2023). — Режим доступа: для авториз. пользователей.

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 самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и

обеспечением доступа к электронной информационно-образовательной среде университета.

Авторы: к.т.н., доцент Матвеев А.В.