МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Брянский государственный технический университет» (БГТУ)

Факультет информационных технологий

(наименование факультета/института)

Кафедра «Системы информационной безопасности»

(наименование кафедры, ответственной за реализацию дисциплины)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 097BC5AE8AD84ED9DE6D4B322263DA87
Владелец: Шкаберин Виталий Александрович
Действителен: с 18.04.2022 до 12.07.2023

УТВЕРЖДАЮ
Первый проректор по учебной работе и цифровизации
_____ В.А. Шкаберин
« 25 » апреля 2023 г.

РАБОЧАЯ ПРОГРАММА
учебной дисциплины

«Организационное и техническое обеспечение защиты КИИ»

(наименование дисциплины)

10.04.01 Информационная безопасность

(код и наименование специальности или направления подготовки)

Организация и технологии защиты информации

(направленность (профиль)/ специализация образовательной программы)

высшее образование – магистратура

(уровень образования)

магистр

(квалификация, присваиваемая по специальности или направлению подготовки)

очная

(форма обучения)

2023

(год набора)

Брянск 2023

Рабочая программа учебной дисциплины
«Организационное и техническое обеспечение защиты КИИ»

(наименование дисциплины)

10.04.01 Информационная безопасность

(код и наименование специальности или направления подготовки)

Организация и технологии защиты информации

(направленность (профиль)/специализация образовательной программы)

Разработал(и):

к.т.н., доцент		М.Ю.Рытов
(должность, ученая степень, ученое звание)	*(подпись)*	*(И.О. Фамилия)*

Рассмотрена и одобрена на заседании кафедры
«Системы информационной безопасности»

(наименование кафедры, ответственной за реализацию дисциплины)

от «3» апреля 2023 г., протокол № 9

Заведующий кафедрой

Зав. кафедрой СИБ, к.т.н., доцент		М.Ю. Рытов
(ученая степень, ученое звание)	*(подпись)*	*(И.О. Фамилия)*

Согласовано:

Заведующий выпускающей кафедрой
Системы информационной безопасности

(наименование выпускающей кафедры)

к.т.н., доцент		М.Ю. Рытов
(ученая степень, ученое звание)	*(подпись)*	*(И.О. Фамилия)*

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Учебная дисциплина «Организационное и техническое обеспечение защиты КИИ» (далее – дисциплина) ориентирована на формирование у обучающихся компетенций в рамках основной профессиональной образовательной программы высшего образования (ОПОП ВО) по направлению подготовки 10.04.01 Информационная безопасность, профиль «Организация и технологии защиты информации».

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины:

– формирование знаний о устройстве и принципах работы систем защиты значимых объектов критической информационной инфраструктуры;

– формирование представления о принципах построения системы защиты значимых объектов критической информационной инфраструктуры;

– получение обучаемыми теоретических знаний о нормативном регулировании в сфере обеспечения информационной безопасности объектов критической информационной инфраструктуры.

Задачей дисциплины является приобретение обучающимися следующих навыков:

а) в организационно-управленческой деятельности:

– планирование и разработка мероприятий по обеспечению безопасности ЗОКИИ;

– реализация мероприятий по обеспечению безопасности ЗОКИИ;

– контроль состояния безопасности ЗОКИИ;

– совершенствование безопасности ЗОКИИ.

б) в проектной деятельности:

– задание требований к обеспечению безопасности значимого объекта КИИ;

– разработка технического задания на создание подсистемы безопасности значимого объекта КИИ;

– проведение анализа угроз безопасности информации в отношении значимых объектов КИИ и выявление уязвимостей в них;

– разработка модели угроз безопасности значимого объекта КИИ;

– разработка проектной (эксплуатационной) документации на значимый объект КИИ (в части обеспечения его безопасности);

в) в эксплуатационной деятельности:

– планирование мероприятий по обеспечению безопасности ЗОКИИ;

– анализ угроз безопасности информации в ЗОКИИ и последствий от их реализации;

– управление (администрирование) подсистемой безопасности ЗОКИИ;

- реагирование на компьютерные инциденты ЗОКИИ;
- информирование и обучение персонала ЗОКИИ;
- внедрение организационных и технических мер по обеспечению безопасности значимого объекта КИИ;
- контроль за обеспечением безопасности ЗОКИИ.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ФГОС

Дисциплина входит в обязательную часть, формируемую участниками образовательных отношений учебного плана образовательной программы и реализуется на 2 курсе в 3 семестре.

Предварительно изучаются дисциплины: Управление информационной безопасностью, Технологии обеспечения информационной безопасности, Технологии и противодействие конкурентной разведки, Информационное противоборство в социотехнических системах, Защита информации ограниченного распространения, Криптографические протоколы и стандарты, Нормативное обеспечение защиты информации, Теоретические основы компьютерной безопасности, Системы автоматизированного проектирования комплексных систем защиты информации, *Комплексные системы защиты информации*

Параллельно изучаются дисциплины: Защищенные информационные системы, Организация аудита информационной безопасности, Компьютерная криминалистика, Аттестация объектов информатизации, *Проектирование информационных систем,* Организационное и техническое обеспечение защиты персональных данных, *Безопасность операционных систем*

Базируются на изучении дисциплины: Управление информационной безопасностью, Технологии обеспечения информационной безопасности, Организация аудита информационной безопасности, Нормативное обеспечение защиты информации, Теоретические основы компьютерной безопасности

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Изучение дисциплины направлено на формирование у обучающихся компетенций ПК-1, представленных в таблице 1.

Таблица 1 – Требования к результатам освоения учебной дисциплины

Код и наименование компетенции	Индикаторы компетенций	В результате изучения учебной дисциплины обучающиеся должны:		
		знать	уметь	владеть
ПК-1. Способен проектировать объекты информатизации в защищенном исполнении	ПК-1.1. Умеет проектировать ОВТ в защищенном исполнении. ПК-1.2. Умеет проектировать выделенные (защищаемые) помещения.	– нормативные правовые акты, методические документы и национальные стандарты в области обеспечения безопасности ЗОКИИ; – основные поня-	– определять категории значимости объектов КИИ; – формировать сведения о результатах присвоения объекту КИИ одной из категорий значи-	– работы с нормативными правовыми актами, методическими документами в области обеспечения безопасности значимых объек-

		тия в области обеспечения безопасности информации, обрабатываемой объектами КИИ; – основы построения систем безопасности ЗОКИИ Российской Федерации и обеспечения их функционирования; – процедуру категорирования объектов КИИ; – процедуры выявления и анализа угроз безопасности информации, обрабатываемой объектом КИИ; – этапы создания подсистемы безопасности значимого объекта КИИ: – порядок оценки угроз безопасности информации и структуру модели угроз безопасности информации значимого объекта КИИ; – общие требования к созданию систем безопасности ЗОКИИ Российской Федерации и обеспечению их функционирования.	мости либо об отсутствии необходимости присвоения ему одной из таких категорий; – определять требования к обеспечению безопасности значимого объема КИИ; – разрабатывать модели угроз безопасности информации значимых объектов КИИ по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности и последствий от их реализации, анализа банка данных угроз безопасности информации; – определять политики управления доступом (дискреционная, мандатная, ролевая, комбинированная); – обосновывать организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта КИИ; – обосновывать виды и типы средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта КИИ; – разрабатывать архитектуру системы безопасности значимого объекта КИИ, включающую состав, места установки, взаимосвязи	тов КИИ; – внедрения организационных и технических мер по обеспечению безопасности значимого объекта КИИ; – работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения значимых объектов КИИ, в том числе зарубежными информационными ресурсами; – планирования мероприятий по обеспечению безопасности значимого объекта КИИ; – анализа угроз безопасности информации в значимом объекте КИИ и последствий от их реализации; – управления (администрирования) подсистемой безопасности значимого объекта КИИ; – управления конфигурацией значимого объекта КИИ и его подсистемой безопасности; – реагирования на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ; – обеспечения действий в нештатных ситуациях в ходе эксплуатации значимого объекта КИИ; – информирования и обуче-

			средств защиты информации; – осуществлять выбор средств защиты информации с учетом категории значимости объекта КИИ, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию; – определять требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности информации и устранение уязвимостей значимого объекта КИИ; – определять меры по обеспечению безопасности при взаимодействии значимого объекта КИИ с иными объектами КИИ. информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями;	ния персонала значимого объекта КИИ; – контроля за обеспечением безопасности значимого объекта КИИ.

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины составляет 3 зачетных единицы (108 академических часов). Распределение трудоемкости дисциплины по видам учебной работы и семестрам представлено в таблице 2.

Таблица 2 – Распределение трудоемкости дисциплины по видам учебной работы и семестрам

Виды учебной работы в соответствии с учебным планом образовательной программы	**Трудоемкость, час.**												
	Всего	**Семестр**											
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**
1. Контактная работа обучающихся с педагогическими работниками, в том числе:	**64**	-	-	64	-		-	-	-	-	-	-	-
1.1. Лекции, час.	**32**	-	-	32	-		-	-	-	-	-	-	-
1.2. Лабораторные работы, час.	**0**	-	-	0	-		-	-	-	-	-	-	-
в том числе в форме практической подготовки													
1.3. Практические занятия, час.	**32**	-	-	32	-		-	-	-	-	-	-	-
в том числе в форме практической подготовки													
2. Самостоятельная работа обучающихся, час.	**35**	-	-	35	-		-	-	-	-	-	-	-
3. Текущий контроль успеваемости и промежуточная аттестация обучающихся, в том числе:	**9**	9											
3.1. Экзамен, семестр		-											
3.2. Зачет, семестр	9	9											
3.3. Зачет с оценкой, семестр		-											
3.4. Курсовой проект (контроль), семестр		-											
3.5. Курсовая работа (контроль), семестр		-											
3.6. Расчетно-графическая работа (контроль), семестр		-											
3.7. Контрольная работа (контроль), семестр		-											
Общая трудоемкость (3 з.е.)	108												

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1. Структура дисциплины

Структура дисциплины представлена в виде тематического плана в таблице 3.

Таблица 3 – Тематический план дисциплины

Наименование раздела (темы) дисциплины	Трудоемкость, час.				
	Всего	**Лекции**	**Лабораторные работы**	**Практические занятия**	**Самостоятельная работа**
Раздел 1. Основы обеспечения безопасности значимых объектов КИИ	28	10	-	10	8
Тема № 1. Правовые основы обеспечения безопасности КИИ Российской Федерации	14	5	-	5	4
Тема № 2 Угрозы безопасности информации, обрабатываемой на объектах КИИ	14	5	-	5	4
Раздел 2. Организация работ по обеспечению безопасности значимого объекта критической информационной инфраструктуры	47	17	-	15	15
Тема № 1. Категорирование объектов КИИ	14	4	-	5	5
Тема № 2. Требования по обеспечению безопасности ЗОКИИ	13	4	-	5	4
Тема № 3. Система безопасности значимого объекта КИИ	8	4	-	2	2
Тема № 4. Стадии (этапы) работ по созданию систем безопасности	12	5	-	3	4
Раздел 3. Контроль за обеспечением безопасности ЗОКИИ в ходе эксплуатации	24	25	-	7	12
Тема № 1. Контроль за обеспечением безопасности ЗОКИИ в ходе эксплуатации	4	5	-	7	12
Зачет, семестр	9	-	-	-	-
Итого	**108**	**32**		**32**	**35**

5.2. Распределение формируемых компетенций по разделам (темам) дисциплины

Распределение формируемых компетенций по разделам дисциплины представлено в таблице 4.

Таблица 4 – Формирование компетенций по разделам дисциплины

Наименование раздела (темы) дисциплины	Код компетенции
	ПК-1

Наименование раздела (темы) дисциплины	Код компетенции
	ПК-1
Раздел 1. Тема № 1. Правовые основы обеспечения безопасности КИИ Российской Федерации	+
Раздел 1. Тема № 2 Угрозы безопасности информации, обрабатываемой на объектах КИИ	+
Раздел 2. Тема № 1. Категорирование объектов КИИ	+
Раздел 2. Тема № 2. Требования по обеспечению безопасности ЗОКИИ	+
Раздел 2. Тема № 3. Система безопасности значимого объекта КИИ	+
Раздел 2. Тема № 4. Стадии (этапы) работ по созданию систем безопасности	+
Раздел 3. Тема № 1. Контроль за обеспечением безопасности ЗОКИИ в ходе эксплуатации	+

5.3. Лекции

Перечень занятий лекционного типа, их содержание и трудоемкость представлены в таблице 5.

Таблица 5 – Тематика и содержание лекций

Наименование темы дисциплины	Тема лекции	Содержание лекции	Трудоемкость, час.
Раздел 1. Тема № 1. Правовые основы обеспечения безопасности КИИ Российской Федерации	Правовые основы обеспечения безопасности КИИ Российской Федерации	1. Нормативно-правовое обеспечения безопасности КИИ Российской Федерации. Ключевые системы информационной инфраструктуры в России. 2. Объекты и субъекты КИИ. Права и обязанности субъектов КИИ. Особенности обеспечения безопасности объектов КИИ Российской Федерации. 3. Полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ. 4. Основные понятия, термины и определения в области обеспечения безопасности значимых объектов КИИ. 5. Система безопасности ЗОКИИ. 6. Права и обязанности субъектов критической информационной инфраструктуры. 7. Государственный контроль в области обеспечения безопасности значимых объектов КИИ. Цели государственного контроля в области обеспечения безопасности значимых объектов КИИ. Виды и периодичность государственного контроля. Основание для проведения плановых и внеплановых проверок. 8. Система нормативных правовых ак-	5

Наименование темы дисциплины	Тема лекции	Содержание лекции	Трудоемкость, час.
		тов по вопросам обеспечения безопасности КИИ Российской Федерации. 9. Организационно-правовые основы аттестации значимых объектов КИИ, лицензирования деятельности в области защиты информации. Система сертификации средств защиты информации. 10. Ответственность за нарушение законодательства о безопасности КИИ Российской Федерации. 11. Обзор подходов к обеспечению безопасности критических информационных инфраструктур в иностранных государствах.	
Раздел 1. Тема № 2 Угрозы безопасности информации, обрабатываемой на объектах КИИ	Угрозы безопасности информации, обрабатываемой на объектах КИИ	1. Объекты КИИ. Объекты защиты. Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления. Типовые объекты КИИ как объекты защиты от угроз безопасности. 2. Понятие и классификация угроз безопасности информации и категорий нарушителей в отношении значимых объектов КИИ. Модель угроз безопасности информации ЗОКИИ. Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. 3. Источники угроз безопасности информации. Уязвимости объектов КИИ, классификация уязвимостей. Способы реализации угроз безопасности информации и их последствия. Банк данных угроз безопасности информации. 4. Типовые способы реализации угроз для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. 5. Типовые негативные последствия для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. 6. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа потенциальных уязвимостей ЗОКИИ, возможных способов реализации угроз безопасности информации и последствий от их реализации.	5

Наименование темы дисциплины	Тема лекции	Содержание лекции	Трудоемкость, час.
		7. Объекты оценки уязвимости: код, конфигурация и архитектура ЗОКИИ для всех программных и программно-аппаратных средств, в том числе средств защиты информации ЗОКИИ. 8. Оценка возможных последствий реализации (возникновения) угроз безопасности информации в значимом объекте КИИ. 9. Структура модели угроз безопасности информации значимого объекта КИИ. 10. Характеристика приказов ФСТЭК России регулирующих обеспечение безопасности критических информационных инфраструктур 11. Обзор приказа ФСТЭК России №227 от 06.12.2017 «Об утверждении Порядка ведения реестра значимых объектов КИИ РФ». 12. Обзор приказа ФСТЭК России №229 от 11.12.2017 «Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ». 13. Обзор приказа ФСТЭК России №235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования». 14. Обзор приказа ФСТЭК России №236 от 22.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий». 15. Обзор приказа ФСТЭК России №239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ». 16. Обзор приказа ФСТЭК России №72 от 26.04.2018 «О внесении изменений в Регламент ФСТЭК»	
Раздел 2. Тема № 1. Категорирование объектов КИИ	Категорирование объектов КИИ	1. Правила и порядок категорирования объектов КИИ, сроки направления сведений о результатах категорирования объекта КИИ в ФСТЭК России. 2. Реестр значимых объектов КИИ. Цель ведения реестра. Сведения, вносимые в реестр значимых объектов КИИ.	5

Наименование темы дисциплины	Тема лекции	Содержание лекции	Трудоемкость, час.
		3. Формирование комиссии по категорированию объектов КИИ Российской Федерации. 4. Определение объектов КИИ Российской Федерации, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов. 5. Определение управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ Российской Федерации. 6. Выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка (критических процессов). 7. Анализ возможных действий нарушителей в отношении объектов КИИ. Анализ угроз безопасности информации и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на объекте КИИ. Оценка возможных последствий компьютерных инцидентов на объектах КИИ. 8. Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значения. 9. Формирование перечня объектов КИИ Российской Федерации, подлежащих категорированию. 10. Оценка в соответствии с перечнем показателей критериев значимости объектов КИИ масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ Российской Федерации 11. Присвоение объектам КИИ Российской Федерации одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости. 12. Подготовка необходимых документов в рамках категорирования объектов КИИ Российской Федерации.	

Наименование темы дисциплины	Тема лекции	Содержание лекции	Трудоемкость, час.
Раздел 2. Тема № 2. Требования по обеспечению безопасности ЗОКИИ	Требования по обеспечению безопасности ЗОКИИ	1. Установление требований по обеспечению безопасности ЗОКИИ. 2. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности ЗОКИИ. 3. Планирование, разработка и совершенствование мероприятий по обеспечению безопасности ЗОКИИ. Сущность, цели и задачи планирования. Порядок разработки, согласования и утверждения плана мероприятий по обеспечению безопасности ЗОКИИ. 4. Реагирование на компьютерные инциденты в ходе эксплуатации ЗОКИИ. 5. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ. Организационные и технические меры, направленные на блокирование (нейтрализацию) угроз безопасности информации: 6. Выбор организационных и технических мер для обеспечения безопасности значимых объектов КИИ. 7. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ. Требования к классам защиты средств защиты информации и средствам вычислительной техники для различных категорий значимости объектов КИИ. Нормативные правовые акты ФСТЭК России, в соответствии с которыми определяются классы защиты средств защиты информации и средств вычислительной техники. Функции безопасности средств защиты информации. Программа и методики испытаний (приемки) средств защиты информации, утверждаемые субъектом КИИ. 8. Нормативные правовые акты ФСТЭК России, в соответствии с которыми определяются классы защиты средств защиты информации и средств вычислительной техники. Функции безопасности средств защиты информации. 9. Программа и методики испытаний (приемки) средств защиты информации, утверждаемые субъектом КИИ.	5
Раздел 2. Тема № 3. Система безопасности	Система безопасности значимого объекта КИИ	1. Цели и задачи системы безопасности ЗОКИИ.	2

Наименование темы дисциплины	Тема лекции	Содержание лекции	Трудоемкость, час.
значимого объекта КИИ		2. Требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования. 3. Требования к силам обеспечения безопасности значимых объектов КИИ. 4. Требования к функционированию подсистемы безопасности в части организации работ по обеспечению безопасности значимых объектов КИИ. 5. Требования к организационно-распорядительным документам по безопасности значимых объектов КИИ. 6. Структура системы безопасности ЗОКИИ. 7. Подготовка необходимых документов в рамках создания систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования.	
Раздел 2. Тема № 4. Стадии (этапы) работ по созданию систем безопасности	Стадии (этапы) работ по созданию систем безопасности	1. Этапы жизненного цикла подсистемы безопасности значимого объекта КИИ. 2. Стадии (этапы) работ по созданию подсистемы безопасности значимого объекта КИИ. 3. Установление требований к обеспечению безопасности значимою объекта КИИ. 4. Разработка организационных и технических мер по обеспечению безопасности значимого объекта КИИ. 5. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта КИИ. 6. Тестирование функционирования подсистемы безопасности значимого объекта КИИ и макетирование элементов системы. 7. Разработка эксплуатационной, организационно-распорядительной документации на значимый объект КИИ и его подсистему безопасности. 8. Предварительные испытания значимого объекта КИИ и его подсистемы безопасности. 9. Опытная эксплуатация значимого объекта КИИ и его подистемы безопасности. 10. Приемочные испытания значимого объекта КИИ и его подсистемы безопасности. 11. Обеспечение безопасности значимого объекта КИИ в ходе его эксплуатации. 12. Обеспечение безопасности значимо-	3

Наименование темы дисциплины	Тема лекции	Содержание лекции	Трудоемкость, час.
		го объекта КИИ при выводе его из эксплуатации.	
Раздел 3. Тема № 1. Контроль за обеспечением безопасности ЗОКИИ в ходе эксплуатации	Контроль за обеспечением безопасности ЗОКИИ в ходе эксплуатации	1. Контроль за обеспечением уровня безопасности ЗОКИИ. Виды контроля (мониторинга) за обеспечением уровня безопасности ЗОКИИ и его системы безопасности. 2. Мониторинг событий безопасности и контроль за действиями персонала в значимом объекте КИИ. 3. Оценка соответствия значимых объектов КИИ требованиям по безопасности. 4. Контроль (анализ) защищенности ЗОКИИ с учетом особенностей его функционирования. 5. Порядок оценки безопасности ЗОКИИ. 6. Анализ и оценка функционирования ЗОКИИ и его системы безопасности, включая выявление, анализ и устранение недостатков в функционировании системы безопасности ЗОКИИ. 7. Принятие решения по результатам контроля за обеспечением уровня безопасности ЗОКИИ о необходимости доработки (модернизации) его системы безопасности. 8. Документирование процедур и результатов контроля за обеспечением уровня безопасности ЗОКИИ. 9. Средства контроля состояния защищенности информации.	7
Итого	–	–	32

5.4. Лабораторные работы

Лабораторные работы по дисциплине не предусмотрены учебным планом образовательной программы (таблица 6).

Таблица 6 – Тематика лабораторных работ

Наименование темы дисциплины	Тема лабораторной работы	Трудоемкость, час.
Итого	–	…

5.5. Практические занятия

Практические занятия по дисциплине предусмотрены учебным планом образовательной программы.

Перечень практических занятий, их содержание и трудоемкость представлены в таблице 7.

Таблица 7 – Тематика и содержание практических занятий

Наименование темы дисциплины	Тема практического занятия	Содержание практического занятия	Трудоемкость, час.
Раздел № 1, Тема № 2	Анализ угроз безопасности информации и уязвимостей программного обеспечения ЗОКИИ с помощью банка данных угроз безопасности информации	Анализ угроз безопасности информации и уязвимостей программного обеспечения ЗОКИИ с помощью банка данных угроз безопасности информации	2
Раздел № 1, Тема № 2	Разработка модели угроз безопасности информации ЗОКИИ	Разработка модели угроз безопасности информации ЗОКИИ	2
Раздел № 2, Тема № 1	Выявление управленческих, технологических, производственных, финансово- экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности	Выявление управленческих, технологических, производственных, финансово- экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности	3
Раздел № 2, Тема № 1	Определение значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов	Определение значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов	3
Раздел № 2, Тема № 1	Формирование акта комиссии по категорированию ЗОКИИ	Формирование акта комиссии по категорированию ЗОКИИ	3
Раздел № 2, Тема № 1	Подготовка сведений о результатах категорирования ЗОКИИ	Подготовка сведений о результатах категорирования ЗОКИИ	3
Раздел № 2, Тема № 2	Разработка плана мероприятий по обеспечению безопасности ЗОКИИ	Разработка плана мероприятий по обеспечению безопасности ЗОКИИ	1
Раздел № 2, Тема № 2	Реагирование на компьютерные инциденты в ходе эксплуатации ЗОКИИ	Реагирование на компьютерные инциденты в ходе эксплуатации ЗОКИИ	1
Раздел № 2, Тема № 2	Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспече-	Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности	3

Наименование темы дисциплины	Тема практического занятия	Содержание практического занятия	Трудоемкость, час.
	нию безопасности ЗОКИИ	ЗОКИИ	
Раздел № 2, Тема № 4	Разработка технического задания (разделов технического задания) на создание СБ ЗОКИИ	Разработка технического задания (разделов технического задания) на создание СБ ЗОКИИ	3
Раздел № 2, Тема № 4	Разработка эксплуатационной, организационно-распорядительной документации на ЗОКИИ и его систему безопасности	Разработка эксплуатационной, организационно-распорядительной документации на ЗОКИИ и его систему безопасности	2
Раздел № 1, Тема № 2	Анализ угроз безопасности информации и уязвимостей программного обеспечения ЗОКИИ с помощью банка данных угроз безопасности информации	Анализ угроз безопасности информации и уязвимостей программного обеспечения ЗОКИИ с помощью банка данных угроз безопасности информации	3
Раздел № 1, Тема № 2	Разработка модели угроз безопасности информации ЗОКИИ	Разработка модели угроз безопасности информации ЗОКИИ	3
Итого	–	…	32

5.6. Самостоятельная работа обучающихся

Вопросы, выносимые на самостоятельное изучение, представлены в таблице 8.

Таблица 8 – Вопросы для самостоятельного изучения дисциплины

Наименование темы дисциплины	Вопросы для самостоятельного изучения темы
Раздел 1. Тема № 1. Правовые основы обеспечения безопасности КИИ Российской Федерации	Самостоятельное изучение вопросов темы. Написание конспекта. Составление глоссария по теме. Проработка и повторение лекционного материала. Изучение рекомендуемой литературы. Подготовка к практическому занятию. Выполнение соответствующих разделов РГР. Подготовка к текущему контролю.
Раздел 1. Тема № 2 Угрозы безопасности информации, обрабатываемой на объектах КИИ	Самостоятельное изучение вопросов темы. Написание конспекта. Составление глоссария по теме. Проработка и повторение лекционного материала. Изучение рекомендуемой литературы. Подготовка к практическому занятию. Выполнение соответствующих разделов РГР. Подготовка к текущему контролю.
Раздел 2. Тема № 1. Категорирование объектов КИИ	Самостоятельное изучение вопросов темы. Написание конспекта. Составление глоссария по теме. Проработка и повторение лекционного материала. Изучение рекомендуемой литературы. Подготовка к практическому занятию. Выполнение соответствующих разделов РГР. Подготовка к текущему контролю.
Раздел 2. Тема № 2. Требования по обеспечению безопасности ЗОКИИ	Самостоятельное изучение вопросов темы. Написание конспекта. Составление глоссария по теме. Проработка и повторение лекционного материала. Изучение рекомендуемой литературы. Подготовка к практическому занятию. Выполнение соответствующих разделов РГР. Подготовка к текущему контролю.

Наименование темы дисциплины	Вопросы для самостоятельного изучения темы
Раздел 2. Тема № 3. Система безопасности значимого объекта КИИ	Самостоятельное изучение вопросов темы. Написание конспекта. Составление глоссария по теме. Проработка и повторение лекционного материала. Изучение рекомендуемой литературы. Подготовка к практическому занятию. Выполнение соответствующих разделов РГР. Подготовка к текущему контролю.
Раздел 2. Тема № 4. Стадии (этапы) работ по созданию систем безопасности	Самостоятельное изучение вопросов темы. Написание конспекта. Составление глоссария по теме. Проработка и повторение лекционного материала. Изучение рекомендуемой литературы. Подготовка к практическому занятию. Выполнение соответствующих разделов РГР. Подготовка к текущему контролю.
Раздел 3. Тема № 1. Контроль за обеспечением безопасности ЗОКИИ в ходе эксплуатации	Самостоятельное изучение вопросов темы. Написание конспекта. Составление глоссария по теме. Проработка и повторение лекционного материала. Изучение рекомендуемой литературы. Подготовка к практическому занятию. Выполнение соответствующих разделов РГР. Подготовка к текущему контролю.

В процессе самостоятельной работы обучающиеся должны принимать решение по рассматриваемой проблеме с минимальным участием педагогического работника. Для решения поставленных задач может использоваться дополнительная литература и источники в информационно-коммуникационной сети «Интернет». Для закрепления пройденного материала педагогическим работником могут выдаваться домашние задания.

В таблице 9 указаны виды самостоятельной работы, выполняемые обучающимися при изучении соответствующих тем дисциплины.

Таблица 9 – Виды самостоятельной работы

Наименование темы дисциплины	Виды самостоятельной работы
Раздел 1. Тема № 1. Правовые основы обеспечения безопасности КИИ Российской Федерации	Написание конспекта. Составление глоссария по теме. Изучение рекомендуемой литературы
Раздел 1. Тема № 2 Угрозы безопасности информации, обрабатываемой на объектах КИИ	Самостоятельное изучение вопросов темы. Написание конспекта. Составление глоссария по теме. Проработка и повторение лекционного материала. Изучение рекомендуемой литературы Подготовка к групповой дискуссии
Раздел 2. Тема № 1. Категорирование объектов КИИ	Самостоятельное изучение вопросов темы. Написание конспекта. Составление глоссария по теме. Проработка и повторение лекционного материала. Изучение рекомендуемой литературы Подготовка к групповой дискуссии
Раздел 2. Тема № 2. Требования по обеспечению безопасности ЗОКИИ	Самостоятельное изучение вопросов темы. Написание конспекта. Составление глоссария по теме.

Наименование темы дисциплины	Виды самостоятельной работы
	Проработка и повторение лекционного материала. Изучение рекомендуемой литературы Подготовка к групповой дискуссии
Раздел 2. Тема № 3. Система безопасности значимого объекта КИИ	Самостоятельное изучение вопросов темы. Написание конспекта. Составление глоссария по теме. Проработка и повторение лекционного материала. Изучение рекомендуемой литературы Подготовка к групповой дискуссии
Раздел 2. Тема № 4. Стадии (этапы) работ по созданию систем безопасности	Составление глоссария по теме. Проработка и повторение лекционного материала. Изучение рекомендуемой литературы Подготовка к групповой дискуссии
Раздел 3. Тема № 1. Контроль за обеспечением безопасности ЗОКИИ в ходе эксплуатации	Написание конспекта. Проработка и повторение лекционного материала. Изучение рекомендуемой литературы Подготовка к групповой дискуссии

Учебным планом в рамках дисциплины не предусмотрено выполнение расчетно-графической работы (РГР)/курсовое проектирование.

Выполнение РГР/курсовое проектирование осуществляется в соответствии с методическими указаниями, содержащимися в соответствующем разделе электронного курса «Основы управления информационной безопасностью» информационно-образовательной среды БГТУ (http://edu.tu-bryansk.ru).

5.7. Организация текущего контроля успеваемости и промежуточной аттестации обучающихся

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины. Формы контрольно-оценочных мероприятий, проводимых в рамках текущего контроля успеваемости, представлены в таблице 10.

Таблица 10 – Формы и периодичность текущего контроля успеваемости

Вид учебной работы	Форма текущего контроля успеваемости	Периодичность осуществления
Практические занятия	Устный экспресс-опрос, экспресс-тестирование.	На каждом занятии
Самостоятельная работа обучающихся	- устная (устный опрос, защита письменной работы, доклада по результатам самостоятельной работы, рефератов и т.д.); - письменная (письменный опрос, выполнение конспектов, глоссариев, расчетно-графической работы / курсового проекта / курсовой работы и т.д.); - тестовая (бланочное или компьютерное тестирование)	В течение семестра

Оценивание промежуточных и окончательных результатов обучения по дисциплине (промежуточная аттестация обучающихся) осуществляется в форме зачета, проводимого в устной / письменной форме. Аттестационное испыта-

ние может включать в себя прохождение теста с использованием технологии компьютерного тестирования. Для уточнения оценки экзаменатор может проводить короткий опрос-собеседование с обучающимся и (или) выдавать ему дополнительные задания.

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе освоения дисциплины применяются следующие образовательные технологии: личностно-ориентированные, активизации деятельности обучающихся, интеллектуальной направленности, проблемного обучения, диалоговые и профессионально-ориентированные (таблица 11).

Таблица 11 – Образовательные технологии, применяемые в ходе преподавания дисциплины

Вид учебной работы	Применяемые образовательные технологии
Лекции	Проблемная лекция. Лекция-визуализация. Лекция-беседа. Лекция-дискуссия.
Практические занятия	Групповые дискуссии. Решение практических задач.
Самостоятельная работа обучающихся	Проработка лекционного материала. Изучение рекомендуемой литературы. Подготовка к дискуссии. Выполнение практического задания Подготовка к лекциям. Подготовка к практическим занятиям. Изучение дополнительной литературы и самостоятельное формирование конспекта. Подготовка к зачету
Консультации	Концентрация внимания на отдельных вопросах. Личностно-ориентированный подход. Диалог.
Промежуточная аттестация обучающихся	Зачет

7. РЕАЛИЗАЦИЯ ДИСЦИПЛИНЫ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И (ИЛИ) ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

В электронной информационно-образовательной среде БГТУ размещается электронный курс дисциплины, включающий в себя:

- сведения об авторе курса;
- краткое описание курса;
- рабочую программу дисциплины;
- полный перечень тем дисциплины;

– презентационные материалы для проведения занятий лекционного типа;

– лекции/краткий конспект лекций по каждой теме;

– методические указания по выполнению каждого практического задания;

– материалы и тестовые задания для текущего контроля успеваемости и промежуточной аттестации обучающихся.

Наименование электронного курса в электронной информационно-образовательной среде БГТУ — «Организационное и техническое обеспечение защиты КИИ» – автор Мусиенко Н. О. разработчика РПД для обучающихся по направлению подготовки 10.04.01 Информационная безопасность, профиль «Организация и технологии защиты информации», форма обучения – очная.

Электронный курс предназначен для обеспечения обучающихся всеми необходимыми учебно-методическими материалами, а также проведения контрольно-оценочных мероприятий в процессе обучения. При необходимости осуществляется файловый обмен отчетами о выполнении обучающимися самостоятельной работы.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

8.2. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

1. Рытов, М.Ю. Обеспечение безопасности критических информационных структур: учеб. пособ. для вузов / М.Ю. Рытов. – Точные наукоемкие технологии, 2021. – 290 с..
2. Рабочая программа учебной дисциплины «Теория систем и системный анализ» для специальности 10.04.01 «Информационная безопасность», магистратура «Организация и технологии защиты информации» [электронный ресурс в ЭБС БГТУ].

8.3. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная литература

1. Макаренко С.И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. – СПб.: Наукоемкие технологии, 2020. – 122 с.
2. Малюк А.А. Основы политики безопасности критических систем информационной инфраструктуры: курс лекций: учебное пособие для вузов/ А.А. Малюк – «Телеком»,2021 – 314с.

3. Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2021. - 352 с.

4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. - М.: ДМК Пресс, 2022. - 416 с.;

5. Язов Ю.К., Соловьев С.В. Защита информации в информационных системах от несанкционированного доступа: пособие. - Воронеж: Кварта, 2020.-440 с.

б) дополнительная литература

1. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: учебное пособие. В 2-х ч. Ч. 1. Правовое обеспечение информационной безопасности. - М.: МИЭТ, 2021. - 184 с.

2. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: учебное пособие. В 2-х ч. Ч. 2. Правовое обеспечение информационной безопасности. - М.: МИЭТ, 2021. - 190 с.

б) справочная литература (Нормативно-правовые акты РФ***)***

1. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне».

2. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

4. Федеральный закон от 4 мая 2011г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

5. Федеральный закон от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации».

6. Перечень сведений, отнесенных к государственной тайне. Утвержден указом Президента Российской Федерации от 30 ноября 1995 г. № 1203.

7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

8. Указ Президента Российской Федерации от 17 марта 2008 г. №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

9. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

10. Указ Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

11. Правила осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Утверждены постановлением Правительства Российской Федерации от 17 февраля 2018 г. № 162.

12. Правила категорирования объектов критической информационной инфраструктуры Российской Федерации. Утверждены постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127.

13. Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения. Утвержден постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127.

14. Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны. Утверждено постановлением Правительства Российской Федерации от 15 апреля 1995 г. № 333.

15. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79.

16. Положение о системе сертификации средств защиты информации. Утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55.

17. Положение о банке данных угроз безопасности информации. Утверждено приказом ФСТЭК России от 16 февраля 2015 г. № 9дсп.

18. Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации. Утвержден приказом ФСТЭК России от 6 декабря 2017 г. № 227.

19. Форма акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Утверждена приказом ФСТЭК России от 11 декабря 2017 г. № 229.

20. Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования. Утверждены приказом ФСТЭК России от 21 декабря 2017 г. № 235.

21. Форма направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Утверждена приказом ФСТЭК России от 22 декабря 2017 г. № 236.

22. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Утверждены приказом ФСТЭК России от 25 декабря 2017 г. №239 (в ред. приказа ФСТЭК России от 9 августа 2018 г. № 138).

23. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Утверждены приказом ФСТЭК России от

14 марта 2014 г. № 31 (в ред. приказа ФСТЭК России от 9 августа 2018 г. № 138).

24. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

25. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам доверенной загрузки). Утверждены приказом ФСТЭК России от 27 сентября 2013 г. № 119дсп.

26. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам контроля съемных машинных носителей информации). Утверждены приказом ФСТЭК России от 28 июля 2014 г. № 87дсп.

27. Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к межсетевым экранам). Утверждены приказом ФСТЭК России от 9 февраля 2016 г. № 9дсп.

28. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

29. Временные требования к средствам антивирусной защиты. Утверждены ФСТЭК России 3 февраля 2012 г.

30. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

31. Базовая модель угроз безопасности информации в ключевых системах информационный инфраструктуры. Утверждена ФСТЭК России 18 мая 2007 г.

32. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.

33. Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи. Утвержден приказом ФСТЭК России от 15 марта 2012 г. № 27.

34. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

35. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

36. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2014.

37. ГОСТР ИСО/МЭК 18028-2008 Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Менеджмент сетевой безопасности. Ростехрегулирование, 2008.

38. ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Ростехрегулирование, 2008.

39. ГОСТ Р ИСО/МЭК ТО 24762-2008 Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения. Ростехрегулирование, 2008.

40. ГОСТ Р ИСО/МЭК ТО 19791-2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем. Ростехрегулирование, 2008.

41. ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения. Росстандарт, 2012.

42. ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний. Росстандарт, 2013.

43. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

44. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. Росстандарт, 2013.

45. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. Росстандарт, 2013.

46. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

47. ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимости. Росстандарт, 2015.

48. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимости информационных систем. Росстандарт, 2015.

49. Профессиональный стандарт «Специалист по технической защите информации». Утвержден приказом Минтруда России от 1 ноября 2016 г. № 599н.

50. Профессиональный стандарт «Специалист по защите информации в автоматизированных системах». Утвержден приказом Минтруда России от 15 сентября 2016 г. № 522н.

51. Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях». Утвержден приказом Минтруда России от 3 ноября 2016 г. № 608н.

52. Правила подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры. Утверждены постановлением Правительства Российской Федерации от 8 июня 2019 г. № 743.

53. Порядок согласования субъектом критической информационной инфраструктуры Российской Федерации с Федеральной службой по техническому и экспортному контролю подключения значимого объекта критической информационной инфраструктуры Российской Федерации к сети связи общего пользования. Утвержден приказом ФСI ЭК России от 28 мая 2020 г. № 75.

54. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну. Утвержден приказом ФСТЭК России от 29 апреля 2021 г. № 77.

55. Перечень информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и Порядок представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Утверждены приказом ФСБ России от 24 июля 2018 г. № 367.

56. Порядок обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядок получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения. Утверждены приказом ФСБ России от 24 июля 2018 г. № 268.

57. Порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации. Утвержден приказом ФСБ России от 19 июня 2019 г. №281.

Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствии компьютерных

атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации. Утвержден приказом ФСБ России от 19 июня 2019 г. № 282.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при изучении дисциплины

1). Сайт научной библиотеки БГТУ (https://libri.tu-bryansk.ru)
2). Электронно-библиотечная система «Лань» (https://e.lanbook.com).
3). Электронно-библиотечная система «IPRbooks» (http://www.iprbookshop.ru).

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и (или) информационных справочных систем

1). Операционная система класса Microsoft Windows.
2). Пакет офисных прикладных программ OpenOffice или Microsoft Office.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для обеспечения обучения необходима следующая материально-техническая база:

- аудитория для проведения лекционных занятий, оборудованная персональными компьютерами, мультимедийным компьютерным проектором, средства звуковоспроизведения (по возможности), проекционным экраном, наличием доступа в информационно-коммуникационную сеть Интернет;
- компьютерный класс для проведения лабораторных работ с установленным комплектом программного обеспечения и доступом в информационно-коммуникационную сеть интернет, оборудованный мультимедийным компьютерным проектором, средства звуковоспроизведения (по возможности), проекционным экраном;
- учебная аудитория, оснащенная комплектом мебели и доской, для проведения консультаций, зачета, зачета с оценкой, экзамена;
- компьютерные классы с постоянным доступом к информационно-телекоммуникационной сети «Интернет», а также читальные залы научной библиотеки БГТУ для самостоятельной работы обучающихся.

10. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Изучение дисциплины инвалидами и лицами с ограниченными возможностями здоровья организуется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

При проведении учебных занятий обеспечивается соблюдение следую-

щих требований:

– учебные занятия проводятся для инвалидов и лиц с ограниченными возможностями здоровья в одной аудитории совместно с обучающимися, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для обучающихся в ходе учебных занятий;

– присутствие ассистента из числа работников БГТУ или привлеченных лиц, оказывающего обучающимся необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с педагогическим работником и т. п.);

– обучающиеся с учетом их индивидуальных особенностей могут пользоваться необходимыми им техническими средствами;

– материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, при отсутствии лифтов аудитория должна располагаться на первом этаже; наличие специальных кресел и других приспособлений).

Университетом созданы специальные условия для получения высшего образования обучающимися с ОВЗ:

1) для лиц с ограниченными возможностями здоровья по зрению:

– наличие альтернативной версии официального сайта организации в сети "Интернет" для слабовидящих;

– размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме (с учетом их особых потребностей) справочной информации о расписании учебных занятий (информация должна быть выполнена крупным рельефно-контрастным шрифтом (на белом или желтом фоне) и продублирована шрифтом Брайля);

– присутствие ассистента, оказывающего обучающемуся необходимую помощь;

– обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

– обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию организации;

2) для лиц с ограниченными возможностями здоровья по слуху:

– дублирование звуковой справочной информации о расписании учебных занятий визуальной (установка мониторов с возможностью трансляции субтитров (мониторы, их размеры и количество необходимо определять с учетом размеров помещения);

– обеспечение надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения Университета, а

также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, локальное понижение стоек-барьеров; наличие специальных кресел и других приспособлений).

11. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

11.1. Методические материалы для педагогических работников

Основными формами организации обучения по дисциплине являются лекции, практические занятия и самостоятельная работа обучающихся.

Организация теоретического обучения предполагает использование инновационных технологий проведения занятий лекционного типа, к которым, в частности, относятся: проблемная лекция, лекция-визуализация, лекция-беседа, лекция-дискуссия, лекция-исследование.

1. *Проблемная лекция* предполагает преимущественно всесторонний анализ исторических и социокультурных, образовательных явлений, научный поиск истины. Проблемная лекция опирается на логику последовательно моделируемых проблемных ситуаций путем постановки проблемных вопросов или предъявления проблемных задач.

2. *Лекция-визуализация* реализует принцип наглядности и учит обучающихся преобразовывать устную и письменную информацию в визуальную форму, что формирует у них профессиональное мышление за счет систематизации и выделения наиболее значимых, существенных элементов содержания обучения.

3. *Лекция-беседа* является наиболее распространенной и сравнительно простой формой активного вовлечения обучающихся в учебный процесс. Такая лекция предполагает непосредственный контакт (диалог) педагогического работника с аудиторией.

4. *Лекция-дискуссия,* в которой в отличие от лекции-беседы педагогический работник при изложении лекционного материала не только использует ответы обучающихся на свои вопросы, но и организует свободный обмен мнениями в интервалах между логическими разделами.

Организация практических занятий по дисциплине направлена на углубление научно-теоретических знаний обучающихся, формирование практических умений и овладение определенными методами самостоятельной работы.

Практические занятия представляют собой занятия по решению различных прикладных задач, образцы которых были даны на лекциях.

Задачи практических занятий:

– помочь обучающимся систематизировать, закрепить и углубить знания теоретического характера;

– научить обучающихся приемам решения задач из предметной области дисциплины;

– способствовать овладению навыками и умениями, входящих в структу-

ру формируемых компетенций в результате освоения дисциплины;

– научить их работать с информацией, книгой, пользоваться справочной и научной и методической литературой;

– формировать умение учиться самостоятельно, т.е. овладевать методами, способами и приемами самообучения, саморазвития и самоконтроля.

Содержание практических работ составляют:

– устные экспресс-опросы;

– групповые дискуссии;

– выполнение практических заданий;

– письменное или компьютерное экспресс-тестирование и др.

Цели практических занятий наилучшим образом достигаются в том случае, если студент предварительно проработал тематику практического занятия. Поэтому преподаватель должен информировать студентов о теме следующего практического занятия, чтобы они могли целенаправленно самостоятельно заниматься в домашних условиях.

Самостоятельная работа обучающихся предполагает аудиторную и внеаудиторную формы организации.

Основными видами самостоятельной работы обучающихся без участия педагогического работника являются: формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.); подготовка к занятиям; составление аннотированного списка статей из соответствующих журналов по отраслям знаний и т.п.; текущий самоконтроль, выполнение расчетно-графической работы/курсового проекта/курсовой работы.

Выполнение РГР/курсового проекта/курсовой работы по дисциплине предусматривает информирование студентов о ее целях, структуре, выдачу методических указаний и задания, разъяснения по выбору варианта, ознакомление с порядком и сроками сдачи готовых материалов, проведение индивидуальных консультаций и разъяснение отдельных вопросов при необходимости.

Основными видами самостоятельной работы обучающихся с участием педагогического работника являются: текущие консультации, прием и разбор домашних заданий и др.

При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, консультации преподавателя и др.

11.2. Методические материалы для обучающихся

Обучающимся, изучающим дисциплину, необходимо знать требования, предъявляемые к их различным видам учебных занятий, в том числе лекционным, практическим, индивидуальным и др. (таблица 12).

Таблица 12 – Методические рекомендации обучающимся по освоению дисциплины

Вид учебной работы	Организация деятельности обучающегося

Вид учебной работы	Организация деятельности обучающегося
Лекции	Изучение дисциплины следует начинать с прослушивания и конспектирования лекций, перечитывать конспект перед выполнением домашних заданий и практическими занятиями. 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. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать педагогическому работнику на консультации, на практическом занятии. Над конспектами лекций надо работать систематически: первый просмотр рекомендуется сделать вечером того же дня, когда была прочитана лекция, затем просмотреть через 3-4 дня, и сделать это еще раз накануне практического занятия.
Практические занятия	Ознакомление с целью и задачами занятия. Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Прослушивание аудио- и видеозаписей по заданной теме. Выполнение (решение) практических заданий и задач по алгоритму, на основе частично поисковой и или исследовательской деятельности и др.
Изучение дополнительной литературы и самостоятельное формирование конспекта	Ознакомление с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующих для запоминания и являющихся основополагающими в конкретной теме. Составление аннотаций к прочитанным источникам и др. Рефлексия собственных достижений
Подготовка к зачету	При подготовке к зачету/зачету с оценкой/экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, шкалу оценивания и др.

12. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

12.1. Виды и средства оценивания результатов освоения дисциплины

Виды и средства оценивания результатов освоения дисциплины представлены в таблице 13.

Таблица 13 – Виды и средства оценивания результатов освоения дисциплины

Код индикатора достижения компетенции	Оценочные средства текущего контроля успеваемости	Оценочные средства промежуточной аттестации обучающихся
ПК-1	Устные экспресс-опросы (все темы	1. Объекты и субъекты КИИ. Права и обязанности субъектов КИИ. 2. Полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ.

Код индикатора достижения компетенции	Оценочные средства текущего контроля успеваемости	Оценочные средства промежуточной аттестации обучающихся
	дисциплины).	3. Основные понятия, термины и определения в области обеспечения безопасности значимых объектов КИИ. 4. Система нормативных правовых актов по вопросам обеспечения безопасности КИИ Российской Федерации. 5. Система безопасности ЗОКИИ. Цели и задачи системы безопасности ЗОКИИ. 6. Права и обязанности субъектов критической информационной инфраструктуры. 7. Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. 8. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей. 9. Оценка возможных последствий реализации угроз безопасности информации в значимом объекте КИИ. 10. Правила и порядок категорирования объектов КИИ. 11. Реестр значимых объектов КИИ. Цель ведения реестра. Сведения, вносимые в реестр значимых объектов КИИ. 12. Формирование комиссии по категорированию объектов КИИ Российской Федерации. 13. Определение критических процессов в рамках выполнения функций (полномочий) субъекта КИИ. 14. Определение объектов КИИ Российской Федерации, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов. 15. Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значения. 16. Выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ Российской Федерации. 17. Формирование перечня объектов КИИ Российской Федерации, подлежащих категорированию. 18. Порядок определения масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ Российской Федерации. 19. Формирование сведений о результатах категорирования объектовКИИ. 20. Установление требований по обеспечению безопасности ЗОКИИ. 21. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности ЗОКИИ. 22. Планирование, разработка и совершенствование мероприятий по обеспечению безопасности ЗОКИИ. 23. Реагирование на компьютерные инциденты в ходе эксплуатации ЗОКИИ. 24. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ. 25. Требования к применяемым средствам защиты информации, к проведению их оценки на соответствие требованиям по безопасности. 26. Требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования. 27. Требования к силам обеспечения безопасности значимых объ-

Код индикатора достижения компетенции	Оценочные средства текущего контроля успеваемости	Оценочные средства промежуточной аттестации обучающихся
		ектов КИИ. 28. Требования к организационно-распорядительным документам по безопасности значимых объектов КИИ. 29. Перечень необходимых документов в рамках создания систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования. 30. Этапы жизненного цикла системы безопасности ЗОКИИ. 31. Стадии (этапы) работ по созданию систем безопасности ЗОКИИ. 32. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта КИИ. 33. Контроль за обеспечением безопасности ЗОКИИ. 34. Мониторинг событий безопасности и контроль за действиями персонала в значимом объекте КИИ. 35. Оценка соответствия значимых объектов КИИ требованиям по безопасности. 36. Документирование процедур и результатов контроля за обеспечением уровня безопасности ЗОКИИ. 37. Ответственность за нарушение законодательства о безопасности КИИ Российской Федерации. 38. Сроки выполнения требований 187-ФЗ. 39. Опишите план мероприятий по подключению Системы безопасности значимых объектов КИИ к ГосСОПКА. 40. Национальный координационный центр по компьютерным инцидента. 41. Порядок обмена информацией о компьютерных инцидентах между субъектами КИИ. 42. Управление инцидентами ИБ в системе безопасности ЗОКИИ.

12.2. Шкала оценивания при текущем контроле успеваемости

Оценивание отдельных видов работ в процессе изучения дисциплины рекомендуется осуществлять с использованием следующей шкалы:

– обучающийся ответил правильно на более, чем 90 % заданных вопросов или вопросов-тестов, выполнил и успешно защитил практические работы, показал отличное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала и т.д. – «отлично» (максимальный уровень освоения компетенций);

– обучающийся ответил правильно на 75-89% заданных вопросов или вопросов-тестов, выполнил и защитил практические работы с незначительными замечаниями, показал хорошее владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала и т.д. – «хорошо» (средний уровень освоения компетенций);

– обучающийся ответил правильно на 60-74% заданных вопросов или вопросов-тестов, выполнил и защитил практические работы со значительными замечаниями, показал удовлетворительное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках

усвоенного учебного материала и т.д. – «удовлетворительно» (минимальный уровень освоения компетенций);

– обучающийся ответил правильно на менее, чем 60% заданных вопросов или вопросов-тестов, не выполнил все или выполнил часть практических работ, не защитил или защитил их со значительными замечаниями, при выполнении задания обучающийся не продемонстрировал уровень самостоятельного владения умениями и навыками при решении профессиональных задач в рамках усвоенного учебного материала и т.д. – «неудовлетворительно» (минимальный уровень освоения компетенций не достигнут).

12.3. Оценивание окончательных результатов обучения по дисциплине

Итоговая оценка по дисциплине определяется с учетом результатов промежуточной аттестации обучающегося (зачета) и оценок, полученных обучающимся в ходе текущего контроля успеваемости в семестре.

12.4. Характеристика результатов обучения

Характеристики результатов обучения по дисциплине в зависимости от полученной обучающимся оценки приведены в таблице 18.

Таблица 18 – Характеристика результатов обучения по дисциплине

Оценка	Характеристика результатов обучения
Зачтено (высокий уровень освоения всех индикаторов достижения компетенций в дисциплине)	Содержание дисциплины освоено полностью, все цели достигнуты, все предусмотренные программой обучения учебные задания выполнены
Зачтено / «Хорошо» (повышенный уровень освоения всех индикаторов достижения компетенций в дисциплине)	Содержание дисциплины освоено полностью, все предусмотренные программой обучения учебные задания выполнены с незначительными замечаниями
Зачтено (базовый уровень освоения всех индикаторов достижения компетенций в дисциплине)	Содержание дисциплины освоено частично, большинство предусмотренных программой обучения учебных заданий выполнено, в них имеются ошибки
Не зачтено (низкий уровень освоения всех индикаторов достижения компетенций в дисциплине)	Содержание дисциплины не освоено, большинство предусмотренных программой обучения учебных заданий либо не выполнены, либо содержат грубые ошибки; дополнительная самостоятельная работа над материалом не привела к какому-либо значительному повышению качества выполнения учебных заданий

12.5. Контрольно-измерительные материалы для текущего контроля успеваемости и промежуточной аттестации обучающихся

Контрольно-измерительные материалы для текущего контроля успеваемости и промежуточной аттестации обучающихся представлены в электронном курсе «Основы управления информационной безопасностью», размещенном в системе электронной поддержки учебных курсов на базе программного обеспе-

чения Moodle со встроенной подсистемой тестирования (edu.tu-bryansk.ru), входящей в состав электронной информационно-образовательной среды БГТУ (http://edu.tu-bryansk.ru) и «Фонд оценочных средств по дисциплине «Основы управления информационной безопасностью».

13. ВОСПИТАТЕЛЬНАЯ РАБОТА

В соответствии с Федеральным законом «Об образовании в Российской Федерации» воспитание - «деятельность, направленная на развитие личности, создание условий для самоопределения и социализации обучающихся на основе социокультурных, духовно-нравственных ценностей и принятых в российском обществе правил и норм поведения в интересах человека, семьи, общества и государства, формирование у обучающихся чувства патриотизма, гражданственности, уважения к памяти защитников Отечества и подвигам Героев Отечества, закону и правопорядку, человеку труда и старшему поколению, взаимного уважения, бережного отношения к культурному наследию и традициям многонационального народа Российской Федерации, природе и окружающей среде».

В учебном процессе воспитательная работа с обучающимися реализуется средствами учебных дисциплин.

Воспитательная деятельность в ходе преподавания дисциплины направленна на формирование у обучающегося системы убеждений, нравственных норм и общекультурных качеств, на оказание им помощи в жизненном самоопределении, нравственном, гражданском и профессиональном становлении, на создание условий для самореализации личности. Воспитательная работа также ориентирует обучающихся на будущую профессиональную деятельность, формируя не только личностные, но и профессионально значимые качества.

Воспитательные задачи во время учебных занятий выполняются в скрытой (контекстной) и открытой (целенаправленной) формах. Скрытая форма воспитательной работы представляет собой воздействие всего хода педагогического процесса на становление личностных качеств обучающихся. Например, соблюдение педагогическим работником трудовой дисциплины, демонстрация преданности науке, заинтересованность в успехе обучающихся, правильная речь, хорошие манеры и т.п. имеют положительное воспитательное значение и формируют у обучающихся добросовестность, исполнительность, трудолюбие, ответственность и другие положительные качества. Обучающиеся неосознанно перенимают данные черты у педагогического работника.

Воспитание в открытой форме – это целенаправленное воздействие содержанием учебной дисциплины на становление личности обучающегося. Например, решение проблем и исследовательская работа формируют у обучающихся умение аргументировать, самостоятельно мыслить, стремление к научному поиску, развивают творчество, профессиональные умения.