Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 12.07.2024 11:25:36
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
«Информационные технологии»
_____ / Д.Г.Демидов /
«15» февраля 2024г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность критической информационной инфраструктуры»

Направление подготовки
10.04.01 Информационная безопасность

Профиль
Системы управления информационной безопасностью

Квалификация
Магистр по защите информации

Формы обучения
Очная

Москва, 2024 г.

Разработчики:

Доцент кафедры «Информационная безопасность», к.т.н, доцент:

 / А.Г.Спеваков /

Согласовано:

Заведующий кафедрой «Информационная безопасность»,

 /И.В. Калуцкий/

Руководитель образовательной программы
Доцент. к.т.н.

 /С.А. Кесель/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине 4
2 Место дисциплины в структуре образовательной программы 5
3 Структура и содержание дисциплины 5
3.1 Виды учебной работы и трудоемкость 5
3.2 Тематический план изучения дисциплины 6
3.3 Содержание дисциплины 7
3.4 Тематика семинарских/практических и лабораторных занятий 10
4 Учебно-методическое и информационное обеспечение 11
4.1. Нормативные документы и ГОСТы 11
4.2. Основная литература 11
4.3. Дополнительная литература 11
4.5. Лицензионное и свободно распространяемое программное обеспечение 12
4.6. Современные профессиональные базы данных и информационные справочные системы 12
5. Материально-техническое обеспечение 12
6. Методические рекомендации 12
6.1. Методические рекомендации для преподавателя по организации обучения 12
6.2. Методические указания для обучающихся по освоению дисциплины 12
7. Фонд оценочных средств 14
7.1. Методы контроля и оценивания результатов обучения 14
7.2. Шкала и критерии оценивания результатов обучения 14
7.3. Оценочные средства 14

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Безопасность критической информационной инфраструктуры» следует отнести совершенствование или получение новых компетенций необходимых для осуществления деятельности по обеспечению безопасности объектов критической информационной инфраструктуры.

К **основным задачам** освоения дисциплины «Безопасность критической информационной инфраструктуры» следует отнести:

- Приобретение знаний о методах планирования и разработки мероприятий по обеспечению безопасности.
- Овладение знаниями о требованиях к силам обеспечения безопасности объектов КИИ, к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности объектов КИИ, к организационно-распорядительным документам по безопасности объектов КИИ.
- Приобретение знаний об анализе угроз безопасности информации в отношении объектов КИИ и выявлении уязвимости в них.
- Приобретение навыков реализации мероприятий по обеспечению безопасности объектов КИИ.
- Овладение принципами контроля состояния безопасности объектов КИИ.
- Освоение методов по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности объектов КИИ.

В результате освоения дисциплины «Безопасность критической информационной инфраструктуры» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код и наименование компетенций	**Индикаторы достижения компетенции**
УК-1. Способность осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИУК-1.1. Знает методы критического анализа, подходы, способствующие разрешению проблемных ситуаций в области безопасности критической инфраструктуры. ИУК-1.2. Умеет критически оценивать компьютерные инциденты и вырабатывать стратегию действий для их устранения. ИУК-1.3. Владеет навыками системного анализа, разработки и внедрения стратегий обеспечения безопасности информационных систем.
ОПК-3. Способность разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	ИОПК-3.1. Знает международные, государственные и отраслевые стандарты в области информационной безопасности ИОПК-3.2. Умеет формулировать требования и разрабатывать техническое задание по защите объекта критической информационной инфраструктуры. Проводить категорирование объектов КИИ. ИОПК-3.3. Владеет навыками разработки организационно-распорядительной документации по обеспечению информационной безопасности. Навыками экспертизы состояния защищенности информации на объекте КИИ.
ПК-9. Способность проводить аудит информационной	ИПК-9.1. Знает каналы утечки информации.

Код и наименование компетенций	Индикаторы достижения компетенции
безопасности информационных систем и объектов информатизации	ИПК-9.2. Умеет проводить инструментальный аудит информационной безопасности информационных систем и объектов информатизации. ИПК-9.3. Владеет методами мониторинга и аудита, выявления угроз информационно безопасности информационных систем и объектов информатизации.
ПК-14. Способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	ИПК-14.1. Знает нормативные и методические документы ФСБ России, ФСТЭК России. ИПК-14.2. Умеет организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности объектов КИИ. ИПК-14.3. Владеет навыками управления организации работ по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности объектов КИИ.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность критической информационной инфраструктуры» относится к числу дисциплин, формируемых участниками образовательных отношений, цикла (Б1.2) основной образовательной программы магистратуры (Б1.2.3).

Дисциплина «Безопасность критической информационной инфраструктуры» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП в обязательной части цикла (Б1.1):

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Организационное и правовое обеспечение информационной безопасности», «Управление информационной безопасностью».

Дисциплина обеспечивает подготовку «Стратегии управления информационной безопасностью» и выпускной квалификационной работы.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часа (лекции – 18 часов, лабораторные занятия – 54 часа, самостоятельная работа студентов – 72 часа, форма контроля – экзамен в 8 семестре).

Структура и содержание дисциплины «Безопасность критической информационной инфраструктуры» по срокам и видам работы отражены в приложении.

3.1 Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			2	
1	**Аудиторные занятия**	**72**	**72**	
	В том числе:			
1.1	Лекции	18	18	
1.2	Семинарские/практические занятия	-	-	
1.3	Лабораторные занятия	54	54	
2	**Самостоятельная работа**	**72**	**72**	
2.1	СРС	72	72	
3	**Промежуточная аттестация**			
	Зачет/диф. зачет/экзамен		экзамен	
	Курсовой проект		-	-
	Итого	**144**	**144**	

3.2 Тематический план изучения дисциплины

(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	**Тема 1. Основы обеспечения безопасности значимых объектов КИИ**	**20**	**6**	**-**	**8**	**-**	**10**
1.1	Тема 1.1 Правовые основы обеспечения безопасности КИИ Российской Федерации	10	2	-	4	-	4
1.2	Тема 1.2. Угрозы безопасности информации, обрабатываемой на объектах КИИ	10	4	-	4	-	6
2	**Тема 2. Организация работ по обеспечению безопасности значимого объекта КИИ**	**80**	**6**	**-**	**30**	**-**	**40**
2.1	Тема 2.1. Категорирование объектов КИИ	10	2	-	4	-	6
2.2	Тема 2.2 Требования по обеспечению безопасности значимых объектов КИИ	10	2	-	4	-	6

2.3	Тема 2.3 Система безопасности значимого объекта КИИ	30	2	-	12	-	16
2.4	Тема 2.4 Стадии (этапы) работ по созданию систем безопасности	30	-	-	10	-	12
3	**Тема 3. Контроль за обеспечением безопасности значимого объекта КИИ**	**44**	**6**	**-**	**16**	**-**	**22**
3.1	Тема 3.1 Контроль за обеспечением безопасности значимого объекта КИИ	44	6		16		22
	Итого	**144**	**18**	**-**	**54**	**-**	**72**

3.3 Содержание дисциплины

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	**Раздел 1 Основы обеспечения безопасности значимых объектов КИИ**	
1.1	Тема 1.1 Правовые основы обеспечения безопасности КИИ Российской Федерации	Объекты и субъекты КИИ. Права и обязанности субъектов КИИ. Особенности обеспечения безопасности объектов КИИ Российской Федерации. Полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Основные понятия, термины и определения в области обеспечения безопасности значимых объектов КИИ. Система безопасности значимого объекта КИИ. Права и обязанности субъектов критической информационной инфраструктуры. 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. Документы в области технического регулирования и стандартизации. Система стандартов в области защиты информации. Организационно-правовые основы лицензирования деятельности в области защиты информации, аттестации объектов информатизации по требованиям безопасности информации. Система сертификации средств защиты информации. Ответственность за нарушение законодательства о безопасности КИИ Российской Федерации.
1.2	Тема 1.2. Угрозы безопасности информации, обрабатываемой на объектах КИИ	Объекты КИИ. Объекты защиты. Понятие и классификация угроз безопасности информации и категорий нарушителей в отношении значимых объектов КИИ. Модель угроз безопасности информации значимого объекта КИИ. Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.

		Источники угроз безопасности информации. Уязвимости объектов КИИ, классификация уязвимостей. Способы реализации угроз безопасности информации и их последствия. Банк данных угроз безопасности информации, включающий базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах. Типовые способы реализации угроз для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. Типовые компьютерные инциденты для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности информации и последствий от их реализации. Объекты оценки уязвимости: код, конфигурация и архитектура значимого объекта КИИ для всех программных и программно-аппаратных средств, в том числе средств защиты информации значимого объекта КИИ. Оценка возможных последствий реализации угроз безопасности информации в значимом объекте КИИ.
2	**Раздел 2. Организация работ по обеспечению безопасности значимого объекта КИИ**	
2.1	Тема 2.1. Категорирование объектов КИИ	Правила и порядок категорирования объектов КИИ, сроки направления сведений о результатах категорирования объекта КИИ в ФСТЭК России. Реестр значимых объектов КИИ. Цель ведения реестра. Сведения, вносимые в реестр значимых объектов КИИ. Формирование комиссии по категорированию объектов КИИ Российской Федерации. Определение объектов КИИ Российской Федерации, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов. Определение управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ Российской Федерации. 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). 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. Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значения. Формирование перечня объектов КИИ Российской Федерации, подлежащих категорированию. Оценка в соответствии с перечнем показателей критериев значимости объектов КИИ масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ Российской Федерации. Присвоение объектам КИИ Российской Федерации одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.

		Подготовка необходимых документов в рамках категорирования объектов КИИ Российской Федерации.
2.2	Тема 2.2 Требования по обеспечению безопасности значимых объектов КИИ	Установление требований по обеспечению безопасности значимого объекта КИИ. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта КИИ. Планирование, разработка и совершенствование мероприятий по обеспечению безопасности значимого объекта КИИ. Сущность, цели и задачи планирования. Порядок разработки, согласования и утверждения плана мероприятий по обеспечению безопасности значимого объекта КИИ. Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ. Организационные и технические меры, направленные на блокирование (нейтрализацию) угроз безопасности информации: – идентификация и аутентификация; – управление доступом; ограничение программной среды; – защита машинных носителей информации; – аудит безопасности; антивирусная защита; – предотвращение вторжений (компьютерных атак); – обеспечение целостности; – обеспечение доступности; – защита технических средств и систем; – защита информационной (автоматизированной) системы (сети) и ее компонентов; – реагирование на инциденты информационной безопасности; – управление конфигурацией; – управление обновлениями программного обеспечения; – планирование мероприятий по обеспечению безопасности; – обеспечение действий в нештатных (непредвиденных) ситуациях; – информирование и обучение персонала. Выбор организационных и технических мер для обеспечения безопасности значимых объектов КИИ. Требования к применяемым средствам защиты информации, к проведению их оценки на соответствие требованиям по безопасности. 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.
2.3	Тема 2.3 Система безопасности значимого объекта КИИ	Цели и задачи системы безопасности значимого объекта КИИ. Требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования. Требования к силам обеспечения безопасности значимых объектов КИИ. Требования к организационно-распорядительным документам по безопасности значимых объектов КИИ. Структура системы безопасности значимого объекта КИИ. Подготовка необходимых документов в рамках создания систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования.

2.4	Тема 2.4 Стадии (этапы) работ по созданию систем безопасности	Этапы жизненного цикла системы безопасности значимого объекта КИИ. Стадии (этапы) работ по созданию систем безопасности значимого объекта КИИ. Тестирование функционирования системы безопасности значимого объекта КИИ и макетирование элементов системы. Разработка эксплуатационной, организационно-распорядительной документации на значимый объект КИИ и его систему безопасности. Внедрение системы безопасности значимого объекта КИИ. Установка и настройка средств защиты информации. Разработка документов по безопасности значимого объекта КИИ. Внедрение организационных мер по обеспечению безопасности значимого объекта КИИ. Предварительные испытания значимого объекта КИИ и его системы безопасности. Опытная эксплуатация значимого объекта КИИ и его системы безопасности. Приемочные испытания значимого объекта КИИ и его системы безопасности.
3	**Раздел 3. Контроль за обеспечением безопасности значимого объекта КИИ**	
3.1	Тема 3.1 Контроль за обеспечением безопасности значимого объекта КИИ	Контроль за обеспечением уровня безопасности значимого объекта КИИ. Виды контроля (мониторинга) за обеспечением уровня безопасности значимого объекта КИИ и его системы безопасности. Мониторинг событий безопасности и контроль за действиями персонала в значимом объекте КИИ. Оценка соответствия значимых объектов КИИ: требованиям по безопасности. Внутренний контроль организации работ по обеспечению безопасности значимых объектов КИИ и эффективности принимаемых организационных и технических мер. Контроль (анализ) защищенности значимого объекта КИИ с учетом особенностей его функционирования. Порядок оценки безопасности значимого объекта КИИ. Анализ и оценка функционирования значимого объекта КИИ и его системы безопасности, включая выявление, анализ и устранение недостатков в функционировании системы безопасности значимого объекта КИИ. Принятие решения по результатам контроля за обеспечением уровня безопасности значимого объекта КИИ о необходимости доработки (модернизации) его системы безопасности. Документирование процедур и результатов контроля за обеспечением уровня безопасности значимого объекта КИИ. Средства контроля состояния защищенности информации.

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Лабораторные занятия

Лабораторная работа 1. Подготовка сведений об организации.
Лабораторная работа 2. Создание комиссии по категорированию.
Лабораторная работа 3. Формирование перечня объектов КИИ.
Лабораторная работа 4. Анализ возможных действий нарушителей в отношении объектов критической информационной инфраструктуры
Лабораторная работа 5. Категорирование объектов КИИ.
Лабораторная работа 6. Выбор средств защиты информации для нейтрализации угроз безопасности информации.
Лабораторная работа 7. Разработка ОРД ЗОКИИ.
Лабораторная работа 8. Настройка средств защиты для обеспечения защищенности объекта КИИ.

4 Учебно-методическое и информационное обеспечение

4.1. Нормативные документы и ГОСТы

1 Федеральный закон от 26 июля 2017 г. N 187-ФЗ https://fstec.ru/files/501/---26--2017--N-187-/902/---26--2017--N-187-.pdf
2 Федеральный закон от 26 мая 2021 г. N 141-ФЗ https://fstec.ru/files/502/---26--2021--N-141-/904/---26--2021--N-141-.pdf
3 ГОСТ Р 7.0.97-2016 Организационно-распорядительная документация. Требования к оформлению документов https://protect.gost.ru/v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=197990
4 Методика оценки угроз безопасности https://fstec.ru/files/495/---5--2021-/891/---5--2021-.pdf
5 Приказ ФСТЭК России от 22 декабря 2017 г. N 236 https://fstec.ru/files/213/----22--2017--N-236/219/----22--2017--N-236.pdf
6 Приказ ФСТЭК России от 21 марта 2019 г. N 59 https://fstec.ru/files/449/-----17--2020--N-240-84-611/804/-----17--2020--N-240-84-611.pdf

4.2. Основная литература

1. Литвиненко, О. В. Правовые аспекты информационной безопасности : учебное пособие / О. В. Литвиненко ; RU. — Новосибирск : СибГУТИ, 2021. — 63 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/257321 (дата обращения: 10.02.2024). — Режим доступа: для авториз. пользователей.
2. Космачева, И. М. Проектирование защищенных баз данных : учебное пособие / И. М. Космачева, Н. В. Давидюк. — Санкт-Петербург : Интермедия, 2021. — 144 с. — ISBN 978-5-4383-0191-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161362 (дата обращения: 10.02.2024). — Режим доступа: для авториз. пользователей.
3. Воробейкина, И. В. Программирование средств защиты информации : учебное пособие / И. В. Воробейкина. — Калининград : БГАРФ, 2021. — 70 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/216425 (дата обращения: 10.02.2024). — Режим доступа: для авториз. пользователей.

4.3. Дополнительная литература

1. Ларина, Т. Б. Администрирование операционных систем. Управление системой : учебное пособие / Т. Б. Ларина. — Москва : РУТ (МИИТ), 2020. — 71 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/175980 (дата обращения: 10.02.2024). — Режим доступа: для авториз. пользователей.
2. Белов, С. В. Изучение основ функционирования систем физической безопасности : учебное пособие / С. В. Белов, Ш. Ш. Иксанов, Н. В. Давидюк ; составители С. В. Белов [и др.]. — Санкт-Петербург : Интермедия, 2020. — 82 с. — ISBN 978-5-4383-0203-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161335 (дата обращения: 10.02.2024). — Режим доступа: для авториз. пользователей.

3. Компьютерная криминалистика : учебное пособие / составители И. А. Калмыков, В. С. Пелешенко. — Ставрополь : СКФУ, 2017. — 84 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155227 (дата обращения: 10.02.2024). — Режим доступа: для авториз. пользователей.

4.4. Электронные образовательные ресурсы

1. ЭОР «Безопасность критической информационной инфраструктуры» [Электронный ресурс] — URL: https://lms.mospolytech.ru/local/crw/course.php?id=12111 (дата обращения: 10.02.2024).

4.5. Лицензионное и свободно распространяемое программное обеспечение

Libreoffice бесплатное ПО, Ubuntu 22.04 LTS бесплатное ПО.

4.6. Современные профессиональные базы данных и информационные справочные системы

1. БДУ ФСТЭК [Электронный ресурс] — URL: https://bdu.fstec.ru/ (дата обращения: 18.02.2024).
2. CVE [Электронный ресурс] — URL: https://www.cve.org/ (дата обращения: 18.02.2024).

5. Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.
Для проведения лабораторных занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

6. Методические рекомендации

6.1. Методические рекомендации для преподавателя по организации обучения

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки магистр 10.04.01 Информационная безопасность.

6.2. Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической и практической подготовки студентов являются лекции и лабораторные работы.

Важным обстоятельством является привлечение внимания студентов к обсуждаемой проблеме, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия требуется предварительная подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю) оповестить студентов о теме занятия, дать перечень литературы по теме, назначить из числа студентов докладчиков и содокладчиков.

При проведении практического занятия преподаватель выполняет, в основном, функции ведущего - следит за регламентом времени, помогает уточнить формулировки, обобщает результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на лабораторном занятии учитывается при определении итоговой оценки его знаний по дисциплине на экзамене.

Самостоятельная работа по дисциплине «Безопасность критической информационной инфраструктуры» предполагает: выполнение студентами домашних заданий. Домашние задания являются, как правило, продолжением практических занятий и содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др.

При выдаче заданий на самостоятельную работу используется дифференцированный подход к студентам. Перед выполнением студентами самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель здания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Текущий контроль осуществляется на лабораторных занятиях, промежуточный контроль осуществляется в тестовой форме.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в устной форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность умений;
- оформление материала в соответствии с требованиями.

7. Фонд оценочных средств

7.1. Методы контроля и оценивания результатов обучения

Методика преподавания дисциплины «Безопасность критической информационной инфраструктуры» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков, обучающихся:

- защита лабораторных работ;
- использование интерактивных форм текущего контроля в форме тестирования;

7.2. Шкала и критерии оценивания результатов обучения

Форма промежуточной аттестации: экзамен.
По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3. Оценочные средства

7.3.1 Текущий контроль
Оценочные средства для текущей аттестации

- Защита отчетов о выполнении лабораторных работ

7.3.2. Промежуточная аттестация

Промежуточная аттестация обучающихся в форме экзамена во 2 семестре проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом тестирования с использованием LMS. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций осуществляются с использованием бально-рейтинговой системы с следующим порядком начисления баллов:

Таблица – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Выполнение работы №1 «Подготовка сведений об организации»	2	Выполнил, но «не защитил»	5	Выполнил, и «защитил»
Выполнение работы №2 «Создание комиссии по категорированию»	2	Выполнил, но «не защитил»	5	Выполнил, и «защитил»
Выполнение работы №3 «Формирование перечня объектов КИИ»	2	Выполнил, но «не защитил»	5	Выполнил, и «защитил»
Выполнение работы №4 «Анализ возможных действий нарушителей в отношении объектов критической информационной инфраструктуры»	3	Выполнил, но «не защитил»	5	Выполнил, и «защитил»
Выполнение работы №5 «Категорирование объектов КИИ»	2	Выполнил, но «не защитил»	5	Выполнил, и «защитил»
Выполнение работы №6 «Выбор средств защиты информации для нейтрализации угроз безопасности информации»	3	Выполнил, но «не защитил»	5	Выполнил, и «защитил»
Выполнение работы №7 «Разработка ОРД ЗОКИИ»	3	Выполнил, но «не защитил»	5	Выполнил, и «защитил»
Выполнение работы №8 «Настройка средств защиты для обеспечения защищенности объекта КИИ»	2	Выполнил, но «не защитил»	5	Выполнил, и «защитил»
СРС	5		8	
Итого	24		48	
Посещаемость	0		16	
Экзамен	0		36	
Итого	24		100	

При итоговом контроле в форме бланкового тестирования студенту предлагается 15 вопросов по различным темам курса. Каждый вопрос оценивается в 4 условных балла. Полученную итоговую сумму условных баллов (максимум 60) переводят в баллы на зачете (максимум 36) путём умножения на 0.6 и округления до целого значения.

Пример тестового задания по дисциплине

1. Субъектом КИИ может являться: ...
1. Автоматизированная система управления
2. Информационная система
3. Индивидуальный предприниматель
4. Государственное учреждение

2. Объектом КИИ может являться: ...
1. Автоматизированная система управления
2. Информационная система
3. Индивидуальный предприниматель
4. Государственное учреждение

3. Субъекты критической информационной инфраструктуры имеют право: ...
1. Разрабатывать и осуществлять мероприятия по обеспечению безопасности значимого объекта критической информационной инфраструктуры
2. Разрабатывать не имеют право, а только осуществлять мероприятия по обеспечению безопасности значимого объекта критической информационной инфраструктуры
3. Только разрабатывать мероприятия по обеспечению безопасности значимого объекта КИИ, а осуществлять мероприятия имеют право только лицензиаты
4. Разрабатывать и осуществлять мероприятия по обеспечению безопасности значимого объекта КИИ субъекты КИИ не имеют права

4. Субъекты критической информационной инфраструктуры обязаны:...
1. Незамедлительно информировать о компьютерных инцидентах НКЦКИ
2. Незамедлительно информировать о компьютерных инцидентах ФСТЭК России
3. Незамедлительно информировать о компьютерных инцидентах ФСБ России
4. Незамедлительно информировать о компьютерных инцидентах МВД России

5. Основными задачами системы безопасности значимого объекта критической информационной инфраструктуры являются: ...
1. Информирование сотрудников о компьютерных инцидентах
2. Восстановление функционирования значимого объекта критической информационной инфраструктуры
3. Недопущение воздействия на систему оповещения ГО и ЧС
4. Непрерывное взаимодействие с удостоверяющим центром

6. Требованиями по обеспечению безопасности ЗОКИИ, предусматриваются: ...
1. Планирование, разработка, совершенствование и осуществление внедрения мероприятий по обеспечению безопасности ЗОКИИ
2. Принятие организационных и технических мер для обеспечения безопасности ЗОКИИ
3. Осуществление полномочий Российской Федерации в области лицензирования для обеспечения безопасности ЗОКИИ
4. Установление параметров и характеристик программных и программно-аппаратных средств, применяемых для обеспечения безопасности ЗОКИИ

7. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры проводится: ...
1. ФСБ России
2. МВД России

3. Департамент информационной безопасности г. Москвы
4. ФСТЭК России

8. Плановая проверка в отношении значимого объекта критической информационной инфраструктуры проводится с интервалом: ...

1. 1 год
2. 2 года
3. 3 года
4. 4 года

9. Основанием для осуществления внеплановой проверки в отношении ЗОКИИ является: ...

1. Возникновение компьютерного инцидента, повлекшего негативные последствия, на значимом объекте критической информационной инфраструктуры
2. Возникновение компьютерного инцидента, на значимом объекте критической информационной инфраструктуры
3. Приказ ФСТЭК, изданный в соответствии с поручением Президента Российской Федерации или Правительства Российской Федерации либо на основании требования прокурора
4. Приказ федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности КИИ

10. По итогам плановой проверки федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ, в отношении ЗОКИИ составляется: ...

1. Договор
2. Предписание
3. Акт
4. Административный протокол

11. Федеральный закон, регулирующий отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации: ...

1. 152-ФЗ
2. 141-ФЗ
3. 131-ФЗ
4. 187-ФЗ

13. Субъект КИИ должен функционировать в сферах: ...

1. Транспорта
2. Образования
3. Торговли
4. Здравоохранения

14. Объектом КИИ может быть автоматизированная система дистанционного обучения ВУЗа...

1. Да
2. Нет

15. Объектом КИИ может быть флюорографический аппарат в поликлинике...

1. Да
2. Нет