МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2021

Форма обучения
очная

Владивосток 2026

Рабочая программа дисциплины (модуля) «Безопасность критической информационной инфраструктуры» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Белёв А.В.

Шумик Е.Г.

Утверждена на заседании кафедры информационной безопасности от 14.05.2026 , протокол № 8

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000FB241F
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

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:

- 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.

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-11 : Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ОПК-11.1к : Анализирует методологический базис теории защиты информации, используемый при разработке программно-аппаратных компонентов комплексных систем обеспечения информационной безопасности	РД4	Знание	принципы построения и функционирования, примеры реализаций современных систем управления базами данных
			РД5	Умение	использовать прикладные решения для обеспечения безопасности КИИ
	ОПК-2 : Способен применять программные средства системного и прикладного назначений, в том числе отечественного	ОПК-2.1к : Понимает принципы работы современных информационных технологий и программных средств, в том	РД1	Знание	методологии и методы проектирования программного обеспечения
			РД2	Умение	проводить выбор эффективных способов

	производства, для решения задач профессиональной деятельности;	числе отечественного производства			реализации структур данных и конкретных алгоритмов при решении профессиональных задач;
			РД3	Навык	участия в экспертизе состояния защищенности информации на объекте защиты

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	**Формирование ценностей**	**Целевые ориентиры**
Формирование гражданской позиции и патриотизма		
Воспитание уважения к Конституции и законам Российской Федерации	Высокие нравственные идеалы	Доброжелательность и открытость
Формирование духовно-нравственных ценностей		
Воспитание чувства долга и ответственности перед семьей и обществом	Взаимопомощь и взаимоуважение	Ответственность
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Высокие нравственные идеалы	Ответственность
Формирование коммуникативных навыков и культуры общения		
Воспитание культуры диалога и уважения к мнению других людей	Взаимопомощь и взаимоуважение	Дисциплинированность

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Безопасность критической информационной инфраструктуры» относится к базовой части дисциплин учебного плана направления «Информационная безопасность автоматизированных систем». Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Основы информационной безопасности». На данную дисциплину опираются «Аудит информационной безопасности», производственная преддипломная практика

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.Б	9	5	91	36	36	0	1	18	89	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Правовые основы обеспечения безопасности КИИ Российской Федерации	РД1, РД4	6	6	0	18	практическое задание, тест
2	Угрозы безопасности информации, обрабатываемой на объектах КИИ	РД2, РД5	6	6	0	18	практическое задание, тест
3	Категорирование объектов КИИ	РД1	6	6	0	18	практическое задание, тест
4	Разработка требований по обеспечению информационной безопасности критически важных объектов.	РД1, РД3, РД4, РД5	6	6	0	18	практическое задание, тест
5	Система защиты информации	РД1, РД2, РД4	6	6	0	18	практическое задание, тест
6	Содержание работ по обеспечению безопасности критических информационных инфраструктур	РД2, РД3, РД4, РД5	6	6	0	18	практическое задание, тест
Итого по таблице			**36**	**36**	**0**	**108**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Правовые основы обеспечения безопасности КИИ Российской Федерации.

Содержание темы: 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.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 2 Угрозы безопасности информации, обрабатываемой на объектах КИИ.

Содержание темы: 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. Оценка возможных последствий реализации угроз безопасности информации в значимом объекте КИИ.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 3 Категорирование объектов КИИ.

Содержание темы: Правила и порядок категорирования объектов КИИ, сроки направления сведений о результатах категорирования объекта КИИ в ФСТЭК России. еестр значимых объектов КИИ. Цель ведения реестра. Сведения, вносимые в реестр значимых объектов КИИ. Формирование комиссии по категорированию объектов КИИ Российской Федерации.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 4 Разработка требований по обеспечению информационной безопасности критически важных объектов.

Содержание темы: Концепция безопасности объекта. Организационные вопросы безопасности. Требования к оформлению концепции обеспечения информационной безопасности объекта. Вопросы безопасности, связанные с персоналом. Требования к классификации и управлению активами, связанными с информационно-телекоммуникационными системами. Вопросы физической защиты и защиты от воздействий окружающей среды. Управление передачей данных и производственной деятельностью.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 5 Система защиты информации.

Содержание темы: Принципы, структурный состав и особенности построения системы защиты информации критически важного объекта. Этапы создания систем защиты информации. Определение информационных и технических ресурсов, подлежащих защите. Выявление полного множества потенциально возможных угроз и каналов утечки информации. Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки. Определение требований к системе защиты. Осуществление выбора средств защиты информации и их характеристик. Внедрение и организация использования выбранных мер, способов и средств защиты. Осуществление контроля целостности и управление системой защиты. .

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 6 Содержание работ по обеспечению безопасности критических информационных инфраструктур.

Содержание темы: Выбор средств защиты информации. Анализ отечественного рынка средств защиты информации. Подходы к выбору средств защиты информации. Программно-технические способы и средства обеспечения информационной безопасности. Сертифицированные отечественные средства предупреждения и обнаружения компьютерных атак и защиты информации, разрабатываемые и производимые лицензиатами федеральных органов исполнительной власти. Системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов. Восстановление работоспособности средств защиты информации, функционирующих на критически важных объектах. Оценка эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. В данной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения и углубления знаний по данной дисциплине целесообразно использовать: научные публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажных носителях. Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение аттестационный мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, кейсовых заданий, самостоятельное изучение некоторых разделов курса Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 4 настоящей РПД.

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания,

методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Елизаров, Д. А. Основы критической информационной инфраструктуры Российской Федерации : учебно-методическое пособие / Д. А. Елизаров, Т. А. Мызникова. — Омск : ОмГУПС, 2023. — 27 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/419264 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.

2. Обеспечение безопасности критической информационной инфраструктуры : учебное пособие / составители А. О. Егорова [и др.]. — Севастополь : СевГУ, 2024. — 110 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/450542 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.

3. Программно-аппаратные средства защиты информации : учебное пособие / С. А. Зырянов, М. А. Кувшинов, И. А. Огнев, И. В. Никрошкин. - Новосибирск : Изд-во НГТУ, 2023. - 80 с. - ISBN 978-5-7782-4905-9. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2246196 (дата обращения: 31.05.2026)

7.2 Дополнительная литература

1. Корниенко, А. А. Категорирование и обеспечение безопасности значимых объектов критической информационной инфраструктуры железнодорожного транспорта : учебное пособие / А. А. Корниенко, А. П. Глухов, С. В. Корниенко. — Санкт-Петербург : ПГУПС, 2024. — 53 с. — ISBN 978-5-7641-1966-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/439472 (дата обращения: 00.00.0000). — Режим доступа: для авториз. пользователей.

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Электронно-библиотечная система "ZNANIUM.COM"
2. Электронно-библиотечная система "ЛАНЬ"
3. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
4. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/
5. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Компьютеры

- Проектор

Программное обеспечение:

- Microsoft Office 2010 Standart

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2021

Форма обучения
очная

Владивосток 2026

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-11 : Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ОПК-11.1к : Анализирует методологический базис теории защиты информации, используемый при разработке программно-аппаратных компонентов комплексных систем обеспечения информационной безопасности
	ОПК-2 : Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.1к : Понимает принципы работы современных информационных технологий и программных средств, в том числе отечественного производства

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ОПК-2 «Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-2.1к : понимает принципы работы современных информационных технологий и программных средств, в том числе отечественного производства	РД 1	Знание	методологии и методы проектирования программного обеспечения	решение тестовых заданий
	РД 2	Умение	проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач;	выполнение практических заданий
	РД 3	Навык	участия в экспертизе состояния защищенности информации на объекте защиты	решение тестовых заданий

Компетенция ОПК-11 «Способен разрабатывать компоненты систем защиты информации автоматизированных систем»

Таблица 2.2 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения

	Код рез-та	Тип рез-та	Результат	
ОПК-11.1к : анализирует методологический базис теории защиты информации, используемый при разработке программно-аппаратных компонентов комплексных систем обеспечения информационной безопасности	РД 4	Знание	принципы построения и функционирования, примеры реализаций современных систем управления базами данных	решение тестовых заданий
	РД 5	Умение	использовать прикладные решения для обеспечения безопасности КИИ	выполнение практических заданий

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : методологии и методы проектирования программного обеспечения	1.1. Правовые основы обеспечения безопасности КИИ Российской Федерации	Тест	Экзамен в устной форме
		1.3. Категорирование объектов КИИ	Тест	Экзамен в устной форме
		1.4. Разработка требований по обеспечению информационной безопасности критически важных объектов.	Тест	Экзамен в устной форме
		1.5. Система защиты информации	Тест	Экзамен в устной форме
РД2	Умение : проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач;	1.2. Угрозы безопасности информации, обрабатываемой на объектах КИИ	Практическая работа	Экзамен в устной форме
		1.5. Система защиты информации	Практическая работа	Экзамен в устной форме
		1.6. Содержание работ по обеспечению безопасности критических информационных инфраструктур	Практическая работа	Экзамен в устной форме
РД3	Навык : участия в экспертизе состояния защищенности информации на объекте защиты	1.4. Разработка требований по обеспечению информационной безопасности критически важных объектов.	Практическая работа	Экзамен в устной форме

		1.6. Содержание работ по обеспечению безопасности критических информационных инфраструктур	Практическая работа	Экзамен в устной форме
РД4	Знание : принципы построения и функционирования, примеры реализаций современных систем управления базами данных	1.1. Правовые основы обеспечения безопасности КИИ Российской Федерации	Тест	Экзамен в устной форме
		1.4. Разработка требований по обеспечению информационной безопасности критически важных объектов.	Тест	Экзамен в устной форме
		1.5. Система защиты информации	Тест	Экзамен в устной форме
		1.6. Содержание работ по обеспечению безопасности критических информационных инфраструктур	Тест	Экзамен в устной форме
РД5	Умение : использовать прикладные решения для обеспечения безопасности КИИ	1.2. Угрозы безопасности информации, обрабатываемой на объектах КИИ	Тест	Экзамен в устной форме
		1.4. Разработка требований по обеспечению информационной безопасности критически важных объектов.	Тест	Экзамен в устной форме
		1.6. Содержание работ по обеспечению безопасности критических информационных инфраструктур	Тест	Экзамен в устной форме

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест 1-5	Практическая работа	Экзамен	Итого
Лекционные занятия	20			80
Практические занятия		60		
Промежуточная аттестация			20	20
Итого	20	60	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала

		, усвоил основную литературу и знаком с дополнительной литературой, рекоме ндованной программой, умеет свободно выполнять практические задания, пред усмотренные программой, свободно оперирует приобретенными знаниями, уме ниями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: осно вные знания, умения освоены, но допускаются незначительные ошибки, неточн ости, затруднения при аналитических операциях, переносе знаний и умений на н овые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворитель но»	Студент демонстрирует сформированность дисциплинарных компетенций: в хо де контрольных мероприятий допускаются значительные ошибки, проявляется о тсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным к омпетенциям, студент испытывает значительные затруднения при оперировани и знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворите льно»	У студента не сформированы дисциплинарные компетенции, проявляется недос таточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворите льно»	Дисциплинарные компетенции не сформированы. Проявляется полное или прак тически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Контрольный тест

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

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, по мнению студента, вариант ответа. В течение семестра проводится 4 теста по 6 темам на лекционных занятиях, в каждом тесте 16 вопросов.

Шкала оценки

Оценка	Баллы	Описание
5	5	Студент допустил не более 2х ошибок
4	4	Студент совершил от 3 до 6 ошибок в ответах на тест
3	2-3	Студент совершил от 7 до 10 ошибок в ответах на тест
2	0-1	Студент совершил 11 и более ошибок в ответах на тест

5.2 Примеры заданий для выполнения практических работ

Практическая работа №1. Подготовка сведений об организации. Создание комиссии по категорированию

Цель работы: подготовить необходимые организационные документы и создать комиссию по категорированию объектов критической информационной инфраструктуры (КИИ).

Практическое задание:

Подготовьте пакет документов, включающих:

Полное наименование организации,

Адрес расположения ключевых подразделений,

Организационно-правовую форму предприятия,

Основные виды деятельности,

Контактные лица и контактные данные руководителей подразделения.

Создайте комиссию по категорированию объектов КИИ. Для этого определите состав членов комиссии (руководители служб ИТ, безопасности, сотрудники технических отделов). Опишите полномочия и обязанности каждого члена комиссии.

Практическая работа №2. Формирование перечня объектов КИИ

Цель работы: определить перечень объектов критически важной инфраструктуры вашей организации, подлежащих защите и оценке риска.

Практическое задание:

Составьте список всех объектов информационно-коммуникационной инфраструктуры вашего предприятия, включая серверы, сети передачи данных, системы управления технологическими процессами и прочие важные элементы.

Проведите классификацию выявленных объектов по уровням значимости и потенциальному ущербу от нарушения их функционирования.

Заполните таблицу, содержащую перечень объектов КИИ с указанием типа объекта, местоположения, назначения и степени важности.

Практическая работа №3. Анализ возможных действий нарушителей в отношении объектов критической информационной инфраструктуры

Цель работы: провести оценку угроз безопасности объектов КИИ путем анализа потенциальных действий злоумышленников.

Практическое задание:

Определите возможные угрозы объектам КИИ, исходя из анализа опыта реальных инцидентов и оценки рисков для отрасли, в которой работает ваша организация.

Разработайте сценарии атак и компрометаций наиболее значимых объектов инфраструктуры. Оцените последствия таких воздействий.

Оформите отчет, содержащий перечень угроз и вероятных последствий нарушений функционирования объектов КИИ.

Практическая работа №4. Категорирование объектов КИИ

Цель работы: присвоение каждому объекту критической информационной инфраструктуры категории опасности согласно действующему законодательству РФ.

Практическое задание:

Проанализируйте ранее сформированный перечень объектов КИИ и проведите их категорирование, основываясь на установленных критериях, утвержденных нормативными актами.

Рассчитайте уровни влияния объектов КИИ на деятельность предприятия и степень возможного ущерба в случае атаки или сбоя.

Присвойте каждому объекту категорию опасности («низкая», «средняя», «высокая») и подготовьте заключение комиссии по результатам категорирования.

Практическая работа №5. Выбор средств защиты информации для нейтрализации угроз безопасности информации

Цель работы: подобрать оптимальные средства защиты информации, способные эффективно нейтрализовать выявленные угрозы.

Практическое задание:

Изучите рынок решений для защиты критической инфраструктуры, выделив подходящие средства и технологии.

Оцените возможности внедрения защитных мер с точки зрения эффективности, стоимости и технической реализуемости.

Выберите конкретные решения для каждого объекта КИИ в зависимости от его категории опасности и вида возможной угрозы.

Практическая работа №6. Разработка организационно-распорядительных документов (ОРД) ЗОКИИ

Цель работы: разработать комплекс нормативных актов и инструкций, обеспечивающих защиту объектов критической информационной инфраструктуры.

Практическое задание:

Составьте регламент внутреннего контроля за соблюдением требований безопасности объектов КИИ.

Разработать инструкции для сотрудников, выполняющих работу с объектами КИИ, включая порядок реагирования на инциденты и правила эксплуатации защищенных систем.

Подготовьте проект приказа руководителя организации о введении в действие разработанных документов и назначении ответственных лиц за обеспечение безопасности объектов КИИ.

Краткие методические указания

На выполнение одной практической работы отводится не менее одного двухчасового занятия. После выполнения каждой практической работы студент должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные задания по теме

Шкала оценки

Оценка	Баллы	Описание
5	8-10	Оценка «отлично» выставляется, если студент выполнил задание, правильно

		применил методы.
4	5-7	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	2-4	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-1	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/ или неверно применил методы необходимые его выполнения.

5.3 Вопросы к экзамену

1. Понятие объекта, критически важного для национальной безопасности государства.

2.Понятия критически важной инфраструктуры, критически важного объекта и информационного критически важного объекта (системы управления критически важным объектом).

3. Классификация критически важных объектов по уровням угроз.

4. Последствия нарушения функционирования критически важных объектов.

5. Доктрина информационной безопасности РФ.

6. Государственные органы РФ, контролирующие деятельность в области защиты информации.

7. Службы, организующие защиту информации на уровне предприятия.

8. Требования по организации обеспечения безопасности информации в критических информационных инфраструктурах.

9. «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007).

10. Уязвимости критически важных объектов. Причины возникновения уязвимостей.

11. Оценка уязвимости критически важных объектов. Степень защищенности критически важных объектов от деструктивного информационного воздействия и актов незаконного вмешательства.

12. Концепция безопасности объекта. Организационные вопросы безопасности.

Требования к оформлению концепции обеспечения информационной безопасности объекта.

13. Вопросы физической защиты и защиты от воздействий окружающей среды

14. Обеспечение безопасности информационных технологий в ходе эксплуатации информационно-телекоммуникационных систем.

15. Архитектура системы защиты информации на критически важном объекте.

16. Выработка политики информационной безопасности предприятия, относящегося к категории критически важного объекта.

17. Политика информационной безопасности. Актуальность политик безопасности. Основные причины создания политик безопасности. Российская специфика разработки политик безопасности.

18. Разработка технических регламентов для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов

19. Разработка и реализация планов восстановления после инцидентов.

20. Разработка плана тренировок, программы тренировок и повышения квалификации персонала, работа которого непосредственно связана с обеспечением безопасности критически важных объектов.

21. Принципы, структурный состав и особенности построения системы защиты информации критически важного объекта.

22. Этапы создания систем защиты информации

23. Содержание работ по обеспечению безопасности информации на критически важном

объекте.

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал исчерпывающе, последовательно, четко и логически стройно его излагает , умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.