

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю

Зам. директора по УР

 Н.А. Андреева

«31» 03 2025 г.

ФТД.01 Основы обеспечения безопасности КИИ Российской Федерации
рабочая программа дисциплины

Кафедра: **Информационная безопасность**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам

Вид учебной работы	ОФ	
	ЗЕ	часов/ семестр
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	1	36/5
Контактная работа, в том числе (по семестрам, курсам):		18/5
Лекции		6/5
Лабораторных работ		
Практических занятий		12/5
Семинаров		
Самостоятельная работа		18/5
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам (курсам)		1/5
Число экзаменов с разбивкой по семестрам (курсам)		

Программу составил:

Профессор кафедры ИБ, д.п.н., доцент Жуковский А.Г.

Рабочая программа дисциплины

«Основы обеспечения безопасности КИИ Российской Федерации»

разработана в соответствии с ФГОС ВО:

направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020г., № 1427.

Составлена на основании учебного плана

направления 10.03.01 Информационная безопасность, профиля «Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)», одобренного Учёным советом СКФ МТУСИ, протокол № 8 от 31.03 2025 г., и утвержденного директором СКФ МТУСИ 31.03 2025 г.

Рассмотрена и одобрена на заседании кафедры

«Информационная безопасность»

Протокол от «31» 03 2025 г. № 8

И.О. Зав. кафедрой



А.Г. Жуковский

1. Цели изучения дисциплины

Целью преподавания дисциплины «Основы обеспечения безопасности КИИ Российской Федерации» является формирование у обучаемых знаний в области основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных и аппаратных средств в сетях и информационных системах.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у обучающегося способности решать профессиональные задачи в соответствии с *эксплуатационным* видом деятельности:

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

Компетенции, формируемые у обучающегося в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ПК-2: Администрирование программно-аппаратных средств защиты информации в компьютерных сетях
Знать: Порядок реализации методов и средств поддержания информационной безопасности объектов КИИ; Виды политик управления доступом и информационными потоками в компьютерных сетях; Источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению; Состав программно-аппаратных комплексов для объектов КИИ; Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации; Правила эксплуатации применяемых программно-аппаратных средств защиты информации на объектах КИИ; Программно-аппаратные средства и методы защиты информации в компьютерных сетях; Нормативные правовые акты в области защиты информации на объектах КИИ; Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры.
Уметь: Оценивать угрозы безопасности информации в компьютерных сетях объектов КИИ; Обосновывать выбор используемых программно-аппаратных средств защиты информации на объектах КИИ; Конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях и на объектах КИИ; Производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях и на объектах КИИ; Оценивать оптимальность выбора программно-аппаратных средств защиты информации Для защиты объектов КИИ.
Владеть: - определением состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях и на объектах КИИ; - разработкой порядка применения программно-аппаратных средств защиты информации в компьютерных сетях и на объектах КИИ; - управлением функционированием программно-аппаратных средств защиты информации в компьютерных сетях и на объектах КИИ; - контролем корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях и на объектах КИИ.

Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.В.06 Введение в профессию
2	Б1.О.27 Основы информационной безопасности.
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.32 Основы управления информационной безопасностью
2	Б1.В.02 Комплексное обеспечение защиты информации объекта информатизации
3	Б1.О.33 Программно-аппаратные средства защиты информации.

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 36 часов, 18 аудиторных часов)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 1, Семестр 4					
Модуль 1. Понятие объекта с критической информационной инфраструктурой. Обеспечение безопасности критической информационной инфраструктуры (6 лек+12 практики) часов					
1.1	Лекция 1. Общая информация. Определение принадлежности к субъектам КИИ	Лек	2	ПК-2	Л1.1 Л1.2
1.2	Лекция 2. Критерии оценки критичности бизнес-процессов. Формирование перечня критических процессов.	Лек	2	ПК-2	Л1.1 Л1.2
1.3	Лекция 3. Обеспечение выполнения требований по безопасности значимых объектов КИИ	Лек	2	ПК-2	Л1.1 Л1.2
1.4	Практическое занятие 1 Взаимодействие субъектов КИИ с ФСТЭК РФ	ПЗ	2	ПК-2	Л3.1 Л3.2 Л3.3
1.5	Практическое занятие 2 Формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию	ПЗ	2	ПК-2	Л3.1 Л3.2 Л3.3
1.6	Практическое занятие 3 Расчет показателей критериев значимости объектов КИИ	ПЗ	2	ПК-2	Л3.1 Л3.2 Л3.3
1.7	Практическое занятие 4 Инвентаризация и категорирование объектов критической информационной инфраструктуры	ПЗ	2	ПК-2	Л3.1 Л3.2 Л3.3
1.8	Практическое занятие 5 Подключение к ГОССОПКА	ПЗ	2	ПК-2	Л3.1 Л3.2 Л3.3

1.9	Практическое занятие 6 Оформление и передача в ФСТЭК России результатов категорирования	ПЗ	2	ПК-2	ЛЗ.1 ЛЗ.2 ЛЗ.3
1.10	1. Федеральный закон от 26 июля 2017 г. N 187-ФЗ О безопасности критической информационной инфраструктуры Российской Федерации 2. Постановление Правительства Российской Федерации от 17 февраля 2018 г. N 162 Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации 3. Приказ ФСТЭК России от 21 декабря 2017 г. N 235 требования к созданию субъектами критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) систем безопасности значимых объектов критической информационной инфраструктуры (далее - системы... 4. Указ Президента Российской Федерации от 5 декабря 2016 г. N 646 инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы... 5. Федеральная служба по техническому и экспортному контролю Информационное сообщение По вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий от 17 апреля 2020 г. N 240/84/611 6. Требования по безопасности информации. Утверждены приказом ФСТЭК России от 30 июля 2018 г. N 132 К средствам защиты информации от воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем Файлы для скачивания: Требования по безопасности информации. 7. Правительство РФ. Постановление от 8 февраля 2018 г. N 127. Об утверждении правил категорирования объектов критической	СРС	18	ПК-2	Л1.1 Л1.2 Л2.1 ЛЗ.1 ЛЗ.2 ЛЗ.3

	информационной инфраструктуры РФ, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений				
	Зачет			ПК-2	Л1.1 Л1.2 Л2.1 Л3.1 Л3.2 Л3.3
Итого 36 часов					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л1.1	Макаренко, С. И.	Аудит безопасности критической инфраструктуры специальными информационными воздействиями : монография	Санкт-Петербург : Научное издательство, 2018.	Э1
Л1.2	Макаренко, С. И.	Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем: учебное пособие. Ч.2: сетевые операционные системы и принципы обеспечения информационной безопасности в сетях : учебное пособие	Санкт-Петербург : Научное издательство, 2020.	Э2
5.1.2. Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	А. И. Елисеев, Д. В. Поляков, В. В. Севенюк, К. В. Стародубов	Основы тестирования КИИ на проникновение : учебное пособие	Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2019.	Э3
5.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л3.1	Н. Забусов	Безопасность КИИ	Компания STEP LOGIC	Э4
Л3.2	ООО «СТЭП ЛОДЖИК»	Методические рекомендации по категорированию объектов КИИ	М.: ООО «СТЭП ЛОДЖИК», 2020. -	Э5
Л3.3	Ассоциация руководителей служб информационной безопасности	Безопасность объектов критической информационной инфраструктуры организации. Общие рекомендации 2019 (версия 2.0)	Москва: АРСИБ, 2019	Э6

5.2. Электронные образовательные ресурсы	
Э1	https://www.iprbookshop.ru/130084.html
Э2	https://www.iprbookshop.ru/130092.html
Э3	https://www.iprbookshop.ru/99777.html
Э4	https://step.ru/innovations/kriticheskaya-informatsionnaya-infrastruktura/
Э5	https://step.ru/upload/pdf/kriticheskaya-informatsionnaya-infrastruktura.pdf
Э6	https://aciso.ru/files/docs/metodichka_2.0.pdf
5.3 Информационно-справочные системы и профессиональные базы данных	
5.3.1	Консультант Плюс – https://www.consultant.ru/
5.3.2	Гарант – https://www.garant.ru/
5.3.2	Консорциум Кодекс – https://docs.cntd.ru/
5.3.3	Научная электронная библиотека – https://www.elibrary.ru/
5.3.4	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)
5.3.5	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)
5.4. Программное обеспечение	
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:	
П.1	MS Word лицензионное
П.2	Power Point лицензионное

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оснащенная интерактивной доской, проектором, ПК (ноутбуком), экраном.
6.2 МТО лабораторных работ и практических занятий	
1	Лаборатория «Программно-аппаратные средства защиты информации», укомплектованная специализированной мебелью, оснащенную программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации,
6.3 МТО рубежных контролей, экзамена	
1	Учебные аудитории, оборудованные компьютерной техникой с возможностью выхода в локальную сеть Филиала и Интернет.
6.4 МТО самостоятельной работы	
1	Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы

Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

8. Методические рекомендации для обучающихся по освоению дисциплины

Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочесть задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «ФТД.01 Основы обеспечения безопасности КИИ Российской Федерации» для использования в 20___/20___ учебном году

Утверждаю

Зам. директора по УР _____
«___» _____ 20___ г.

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения: очная

(Возможны следующие варианты):

а) Рабочая программа действует без изменений.

б) В рабочую программу вносятся следующие изменения:

1)

2)

3)

Разработчик (и): _____

(ФИО, ученая степень, ученое звание)

«___» _____ 20___ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБ

Протокол № _____ от «___» _____ 20___ г.

Заведующий кафедрой _____

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	Уровень освоения компетенции	Критерии оценивания
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не достигнут	Обучающийся обнаруживает пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не знаком с рекомендованной литературой, не может исправить допущенные ошибки. Как

		правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.
--	--	---

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания
ПК-2		
Знать:		
Порядок реализации методов и средств поддержания информационной безопасности объектов КИИ; Виды политик управления доступом и информационными потоками в компьютерных сетях; Источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению; Состав программно-аппаратных комплексов для объектов КИИ; Методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации; Правила эксплуатации применяемых программно-аппаратных средств защиты информации на объектах КИИ; Программно-аппаратные средства и методы защиты информации в компьютерных сетях; Нормативные правовые акты в области защиты информации на объектах КИИ; Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры.	Контрольная работа	Модуль 1 0÷40 «Неудовлетворительно» - 0-15 «Удовлетворительно» - 16-24 «Хорошо» - 25-32 «Отлично» - 33-40
Уметь		
Оценивать угрозы безопасности информации в компьютерных сетях объектов КИИ; Обосновывать выбор используемых программно-аппаратных средств защиты информации на объектах КИИ; Конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях и на объектах КИИ; Производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях и на объектах КИИ; Оценивать оптимальность выбора программно-аппаратных средств защиты информации Для защиты	Практическое занятие 1-6	Модуль 1 0÷10 за каждое ПЗ сумма баллов за 6 ПЗ 60 баллов «Неудовлетворительно» - 0-2 «Удовлетворительно» - 4-3 «Хорошо» - 5-7 «Отлично» - 8-10

объектов КИИ.		
Владеть		
Определением состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях и на объектах КИИ; Разработкой порядка применения программно-аппаратных средств защиты информации в компьютерных сетях и на объектах КИИ; Управлением функционированием программно-аппаратных средств защиты информации в компьютерных сетях и на объектах КИИ; Контроль корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях и на объектах КИИ.	Практическое занятие 1-6	Модуль 1 0÷10 за каждое ПЗ сумма баллов за 6 ПЗ 60 баллов «Неудовлетворительно» - 0-2 «Удовлетворительно» - 4-3 «Хорошо» - 5-7 «Отлично» - 8-10
Зачет		41-100 баллов

1.3 Оценочные материалы для текущего контроля и промежуточной аттестации: типовые контрольные задания, иные материалы

1.3.1 Оценочные средства текущего контроля для очной формы обучения

Модуль 1 (100 баллов):

Модуль содержит 3 лекционных занятия и 6 практических занятий. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 40. За выполненные практические работы обучающийся получает максимум 60 баллов. Общее максимальное количество баллов за модуль 1 составляет 100.

Вопросы для контрольной работы (ПК-2):

1. Угрозы конфиденциальной информации
2. Действия, приводящие к неправомерному овладению конфиденциальной информацией
3. Правовая защита
4. Организационная защита
5. Инженерно-техническая защита
6. Кто попадает под действие закона о КИИ
7. Критическая информационная инфраструктура- это
8. Какие органы производят регулирование требований закона
9. Обязанности субъектов КИИ
10. Владельцы значимых объектов КИИ: должны
11. Состав комиссии по категорированию
12. Указать порядок категорирования
13. Процесс категорирования объектов КИИ включает следующие шаги.
14. Указать содержание акта категорирования объекта КИИ
15. Сведения, направляемые во ФСТЭК по КИИ
16. Перечислить показатели критериев значимости объектов КИИ
17. Состав системы безопасности значимого объекта КИИ
18. Требования к средствам обеспечения безопасности значимого объекта КИИ

19. Мероприятия по обеспечению безопасности на стадиях жизненного цикла объектов КИИ
20. Организационные и технические меры
21. Порядок осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ
22. Ответственность за нарушения ИБ КИИ

Темы практических занятий (ПК-2):

Практическое занятие 1. Типология объектов КИИ

Практическое занятие 2. Создание комиссии по категорированию

Практическое занятие 3. Формирование перечня критических процессов

Практическое занятие 4. Формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию

Практическое занятие 5. Обеспечение выполнения требований по безопасности значимых объектов КИИ (ПК-2):

Практическое занятие 6. Категорирования объектов критической информационной инфраструктуры (ПК-2):

1.3.2 Вопросы, выносимые на зачет по дисциплине «Основы информационной безопасности» (ПК-2) (промежуточная аттестация)

1. Угрозы конфиденциальной информации
2. Действия, приводящие к неправомерному овладению конфиденциальной информацией
3. Правовая защита
4. Организационная защита
5. Инженерно-техническая защита
6. Кто попадает под действие закона о КИИ
7. Критическая информационная инфраструктура- это
8. Какие органы производят регулирование требований закона
9. Обязанности субъектов КИИ
10. Владельцы значимых объектов КИИ: должны
11. Состав комиссии по категорированию
12. Указать порядок категорирования
13. Процесс категорирования объектов КИИ включает следующие шаги.
14. Указать содержание акта категорирования объекта КИИ
15. Сведения, направляемые во ФСТЭК по КИИ
16. Перечислить показатели критериев значимости объектов КИИ
17. Состав системы безопасности значимого объекта КИИ
18. Требования к средствам обеспечения безопасности значимого объекта КИИ
19. Мероприятия по обеспечению безопасности на стадиях жизненного цикла объектов КИИ
20. Организационные и технические меры
21. Порядок осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ
22. Ответственность за нарушения ИБ КИИ

2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Порядок и методика проведения текущего контроля и промежуточной аттестации

Предусмотрены следующие виды контроля:

- текущий контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;
- текущий контроль по каждому модулю – в форме отчетов по лабораторным работам и практическим занятиям для оценки практических навыков;
- промежуточная аттестация по дисциплине – в форме зачета.

Текущий контроль успеваемости в форме защиты лабораторных и практических проводится в два этапа:

- 1-й этап: допуск к выполнению лабораторной работы – проводится в форме письменной «летучки» (5-10 мин) с целью контроля знаний обучающихся теоретической части лабораторной работы и готовности к выполнению практических исследований;
- 2-й этап выполняется по окончании каждой лабораторной работы (практического занятия) в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки обучающимся практических навыков исследования на аппаратуре.

Контрольные работы выполняются в виде короткого письменного ответа на один вопрос, изученный на предыдущей лекции в начале каждой последующей лекции. Ответ на вопрос дается в течение 5-10 минут. Таким образом, после лекционного курса каждого модуля формируется общая оценка за теоретические знания.

С целью повышения качества обучения за счет побуждения обучающихся к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности обучающихся в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимся баллы в рамках текущего контроля переводятся в оценку на зачете в соответствии со следующей шкалой:

- «не зачтено» - от 0 до 40 от максимального количества баллов;
- «зачтено» - от 41 до 100 максимального количества баллов.

Соотношения максимального количества баллов, полученных обучающимся по блокам модулей, показаны в Таблице .

Таблица - Распределение баллов по модулям дисциплины «Основы обеспечения безопасности КИИ Российской Федерации»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок
Модуль 1	100	40	60
Зачет	100		

Теоретический блок оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения заданий на практических занятиях.

На зачете производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуются формировать вопросы в билетах таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

3 Промежуточная аттестация

Промежуточная аттестация проводится в форме зачета. Зачет проводится по расписанию в устном виде по билетам к зачету. Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

Образец билета к зачету

	МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»	Утверждаю Зав. кафедрой «ИБ» _____ Жуковский А.Г. «___» _____ 20__ г.
Направление подготовки: 10.03.01 Информационная безопасность Курсы: 2 Дисциплина: Основы обеспечения безопасности КИИ Российской Федерации		
Билет №1 1. Понятие и сущность защиты информации (ЗИ). Назначение ЗИ. Задачи ЗИ. Принципы организации ЗИ. 2. Компьютерные вирусы и механизмы борьбы с ними. Профилактика заражения вирусами компьютерных систем. «___» _____ 20__ г. Профессор кафедры «ИБ» _____ Жуковский А.Г.		

Один комплект отпечатанных билетов к зачету, подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину

Вопросы для тестирования в рамках проведения независимой внутренней оценки качества образования (ПК-2)

Один комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

- 1) К правовым методам, обеспечивающим информационную безопасность, относятся:
 - Разработка аппаратных средств обеспечения правовых данных
 - Разработка и установка во всех компьютерных правовых сетях журналов учета действий
 - Разработка и конкретизация правовых нормативных актов обеспечения безопасности
- 2) Основными источниками угроз информационной безопасности являются все указанное в списке:
 - Хищение жестких дисков, подключение к сети, инсайдерство
 - Перехват данных, хищение данных, изменение архитектуры системы
 - Хищение данных, подкуп системных администраторов, нарушение регламента работы
- 3) Виды информационной безопасности:
 - Персональная, корпоративная, государственная
 - Клиентская, серверная, сетевая
 - Локальная, глобальная, смешанная

- 4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
- несанкционированного доступа, воздействия в сети
 - инсайдерства в организации
 - чрезвычайных ситуаций
- 5) Основные объекты информационной безопасности:
- Компьютерные сети, базы данных
 - Информационные системы, психологическое состояние пользователей
 - Бизнес-ориентированные, коммерческие системы
- 6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
 - Техническое вмешательство, выведение из строя оборудования сети
 - Потеря, искажение, утечка информации
- 7) К основным принципам обеспечения информационной безопасности относится:
- Экономической эффективности системы безопасности
 - Многоплатформенной реализации системы
 - Усиления защищенности всех звеньев системы
- 8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
 - органы права, государства, бизнеса
 - сетевые базы данных, файерволы
- 9) К основным функциям системы безопасности можно отнести все перечисленное:
- Установление регламента, аудит системы, выявление рисков
 - Установка новых офисных приложений, смена хостинг-компаний
 - Внедрение аутентификации, проверки контактных данных пользователей
- 10) Принципом информационной безопасности является принцип недопущения:
- Неоправданных ограничений при работе в сети (системе)
 - Рисков безопасности сети, системы
 - Презумпции секретности
- 11) Принципом политики информационной безопасности является принцип:
- Невозможности миновать защитные средства сети (системы)
 - Усиления основного звена сети, системы
 - Полного блокирования доступа при риск-ситуациях
- 12) Принципом политики информационной безопасности является принцип:
- Усиления защищенности самого незащищенного звена сети (системы)
 - Перехода в безопасное состояние работы сети, системы
 - Полного доступа пользователей ко всем ресурсам сети, системы
- 13) Принципом политики информационной безопасности является принцип:
- Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
 - Одноуровневой защиты сети, системы
 - Совместимых, однотипных программно-технических средств сети, системы
- 14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
 - Логические закладки («мины»)
 - Аварийное отключение питания
- 15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
 - Сохранить приложение в папке «Спам», выяснить затем IP-адрес генератора спама
 - Удалить письмо с приложением, не раскрывая (не читая) его
- 16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения

- Секретность информации определена скоростью передачи данных
- Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь
- Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелегального ПО
- Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
- Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет
- Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризующаяся:

- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

- Целостность
- Доступность
- Актуальность

23) Угроза информационной системе (компьютерной сети) – это:

- Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной
- Правовой
- Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке:

- Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

- Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

- Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- Аудит, анализ уязвимостей, риск-ситуаций

- 29) Очень сложные пароли гарантируют 100% защиту?
А.Нет
Б.Да, если после работы полностью очищать куки и не хранить пароль на компьютере
В.Да, если пароль не сохранен на компьютере
- 30.Какие вирусы активизируются после включения ОС?
А.Снифферы
Б.Загрузочные
В.Трояны
Г.Черви
- 31.Представляют ли угрозу вирусы для крупных компаний?
А.Нет
Б.Да, представляют
В.Скорее нет. В крупных компаниях развита система безопасности
Г.Если компания обладает сотрудниками занимающимися безопасностью сети, вирусы не могут нанести такому предприятию вреда
- 32.С чем связана атака введением произвольных запросов в базу данных?
А.Уязвимость SQL Injection
Б.Сбой Denial of Service
В.Ошибка Denial of Service
Г.Неполадка PHP Include
- 33.Фильтрация контента, для чего она служит?
А.Защищает от скрытой загрузки вредоносного программного обеспечения +
Б.Помогает быстро находить в сети требуемый контент сохраняя при этом много драгоценного времени
В.Отключает назойливую рекламу
Г.Отсеивает поисковый спам
- 34.Какой уровень безопасности трафика обеспечивает WPA2?
А.Высокий
Б.Низкий
В.Достаточный для домашней сети
Г.Средний
- 35.Сколько минимально символов должен содержать безопасный пароль, состоящий из латинских строчных букв?
А.15
Б.8
В.10
Г.6
- 36.Какую угрозу можно назвать преднамеренной? Сотрудник:
А.Открыл письмо содержащее вредоносное ПО
Б.Ввел неправильные данные
В.Совершил не авторизованный доступ
Г.Включил компьютер без разрешения
37. Безопасно ли вводить пароли простым копированием?
А.Безопасно если это мой компьютер
Б.Да
В.Безопасно если после работы очистить куки
Г.Нет
- 38.Какую защиту необходимо использовать против программы iSteg или ее аналогов?
А.Шифровать трафик
Б.Использовать очень сложные пароли
В.Устанавливать только лицензионные антивирусы
Г.Не пользоваться Wi-fi
39. Что может привести к заражению компьютера?
А.Получение сообщения по электронной почте
Б.Загрузка пиратского ПО

- В.Создание нового файла
- Г.Отправка сообщения по электронной почте

40. Что такое Brute Force?

- А.Взлом методом заражения системы через вредоносный файл
- Б.Метод заставляющий пользователя самому раскрыть конфиденциальную информацию
- В.Получение конфиденциальной информации с компьютера методом электронной рассылки
- Г.Взлом методом перебора паролей

41. В каком блок файле autorun.inf чаще всего прописывается вредоносная программа?

- А.Open
- Б.Setup
- В.Download
- Г.Dll

42. Как называется преднамеренно внесенный в программное обеспечение объект, приводящий к действиям программного обеспечения не предусмотренным производителем, приводящим к нарушению конфиденциальности и целостности информации?

- А.Троян
- Б.Бэкдор
- В.Закладка
- Г.Вирус

43. Безопасно ли сохранять пароли в автозаполнении браузера?

- А.Да, если пароль к входу в систему знаю только я один
- Б.Нет
- В.Да, если этим компьютером пользуюсь только я один
- Г.Да

44. Для чего служит DLP? Система выполняет функцию:

- А.Защита компьютера от вирусов
- Б.Выполняет функцию безопасного ввода паролей
- В.Предотвращает утечку информации с компьютера
- Г.Предупреждает пользователя о попытках взлома и хакерских атаках

45. Антивирус полностью защищает компьютер от вирусов и атак при работе в сети. Вы согласны с этим?

- А.Нет
- Б.Да, если это лицензионный антивирус известного производителя
- В.Защищает совместно с включенным брандмауэром
- Г.Да

46. Самый лучший способ хранения паролей в информационной системе?

- А.Хеширование
- Б.Вообще не сохранять
- В.Архивирование
- Г.Хранить только с включенным брандмауэром

47. Какое минимальное количество символов должен содержать пароль входа субъектов в систему АС, при классе защищенности 1А?

- А.12
- Б.8
- В.10
- Г.15

48. На каких системах более динамично распространяются вирусы?

- А.Linux
- Б.MacOS
- В.Android
- Г.Windows

49. Самая массовая угроза компьютерной безопасности, это:

- А.Спам
- Б.Трояны

В.Черви
Г.Шпионские программы

50. Если компьютер работает в нормальном режиме, означает ли это что он не заражен?

- А.Нет
- Б.Если не изменилась скорость работы, компьютер совершенно чист
- В.Да
- Г.Если антивирус ничего не показывает компьютер чист

51. Установка одновременно нескольких антивирусных программ повышает защищенность. Вы согласны с этим?

- А.Да
- Б.Да, если это антивирусы от известных производителей
- В.Да, если это антивирусы одного производителя
- Г.Нет

52. Что чаще всего используют злоумышленники при атаке на компьютеры должностных лиц и руководителей крупных компаний?

- А.Фишинг
- Б.Спам
- В.Загрузка скрытого вредоносного ПО
- Г.DDoS атаки

53. Как гарантировать 100% защищенность компьютера от заражения вирусами в сети?

- А.Включить брандмауэр
- Б.Установить новое программное обеспечение
- В.Таких гарантий нет
- Г.Посещать только сайты известных брендов

54. Что необходимо выполнять для контроля безопасности электронной почты?

- А.Часто сменять пароли
- Б.Проверять страницу посещения
- В.Регистрировать почтовый ящик только в известных системах
- Г.Использовать сложные пароли

55. Что такое Firewall, для чего он нужен?

- А.для фильтрации трафика
- Б.для очистки компьютера
- В.для быстрого и безопасного поиска информации
- Г.для форматирования

56. Обеспечивает ли форматирование жесткого диска полное избавление от вирусов?

- А.Обеспечивает полностью
- Б.Обеспечивает если выполнено быстрое форматирование
- В.Нет
- Г.Обеспечивает при низкоуровневом форматировании

57. Можно ли хранить важную информацию на жестком диске компьютера, в том числе пароли?

- А.Да, если это мой личный компьютер
- Б.Да
- В.Нет
- Г.Да, если компьютер не подключен к интернету

58. Если, не нажимая на иконки просто просмотреть подозрительный сайт, ничего не произойдет. Вы согласны?

- А.Нет. Заражение может произойти, даже если вы просто посмотрели информацию с экрана, при этом ничего не нажимая
- Б.Да, простой просмотр не наносит никакого вреда
- В.Да, заражение происходит только после кликов, чем запускается вирусная программа.

59. Что такое государственная тайна?

- 1) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ
- 2) Сведения о состоянии окружающей среды

- 3) Все сведения, которые хранятся в государственных базах данных
- 4) Сведения о состоянии здоровья президента РФ
- 5) Конкретные сведения, в отношении которых компетентные органы и их должностные лица приняли решение об их отнесении к государственной тайне

60. Что такое коммерческая тайна?

- 1) Информация, имеющая действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам
- 2) Информация, к которой нет доступа на законном основании
- 3) Информации, обладатель которой принимает меры к охране ее конфиденциальности
- 4) Информация, содержащая в учредительных документах
- 5) Информация, содержащая в годовых отчетах, бухгалтерских балансах, формах государственных статистических отчетов

Методика оценивания знаний

Максимальное время выполнения теста - 60 минут.

Количество вопросов в тестовом задании - 60.

Для проведения контроля знаний компьютер формирует в случайном порядке тестовые вопросы.

При прохождении тестового контроля знаний обучающийся должен выбрать один или несколько правильных ответов на один из вопросов тестового задания.

В случае правильного ответа на 49 и более тестовых вопросов (>81%) обучающийся подтверждает освоение компетенций с оценкой «отлично», при ответе на 48-37 вопросов (61-80%) обучающийся подтверждает освоение компетенций с оценкой «хорошо», при ответе на 36-25 вопросов (41-60%) обучающийся подтверждает освоение компетенций с оценкой «удовлетворительно», при ответе менее чем на 25 вопросов (<41%) обучающийся не подтверждает необходимый уровень знаний и оценивается неудовлетворительно.

4 Тестовые задания по дисциплине «ФТД.01 Основы обеспечения безопасности КИИ Российской Федерации»

Тестовые задания позволяют оценить уровень сформированности компетенции ПК-2 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень (Блок А) содержит примерно 50 % заданий.

Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень (Блок Б) в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень (Блок В) в среднем составляют – 15 % заданий.

В задании используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий по компетенции ПК-2 равно 20.

Ключи к ответам представлены в отдельной таблице.

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Тексты заданий
1	К правовым методам, обеспечивающим информационную безопасность, относятся: 1. Разработка аппаратных средств обеспечения правовых данных 2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий 3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности
2	Основные объекты информационной безопасности: 1. Вычислительные системы, компьютерные сети, базы данных 2. Информационные системы, психологическое состояние пользователей 3. Бизнес-ориентированные, коммерческие системы
3	Основными рисками информационной безопасности являются: 1. Искажение, уменьшение объема, перекодировка информации 2. Техническое вмешательство, выведение из строя оборудования сети 3. Потеря, искажение, утечка информации
4	К критической информационной инфраструктуре (КИИ) могут относиться: 1. Информационные системы; 2. Информационно-телекоммуникационные сети; 3. Автоматизированные системы управления; 4. Сети электросвязи; 5. Домашние компьютеры; 6. Компьютерные классы
5	В течение какого количества дней после утверждения перечень объектов КИИ в печатном и электронном виде направляется в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры. 1. 5 2. 7 3. 10 4. 30

№ задания	Тексты заданий
6	Комиссию по категорированию может возглавлять 1. Руководитель субъекта критической информационной инфраструктуры 2. Уполномоченное руководителем критической информационной инфраструктуры лицо. 3. Представитель государственных органов 4. Представитель российских юридических лиц
7	С какой периодичностью осуществляется пересмотр установленных категорий значимости или решений об отсутствии необходимости присвоения объектам таких категорий 1. 1 раз в 3 года 2. 1 раз в 5 лет 3. 1 раз в 10 лет 4. 1 раз в 15 лет
8	К нормативным правовым актам, посвященным критической информационной инфраструктуре относятся: 1. Федеральный закон от 26 июля 2017 г. N 187-ФЗ 2. Постановление Правительства Российской Федерации от 17 февраля 2018 г. N 162 3. Постановление Правительства Российской Федерации от 8 февраля 2018 г. N 127 4. Приказ ФСТЭК России от 20 апреля 2023 г. N 69 5. Приказ ФСТЭК России от 21 декабря 2017 г. N 235 6. Приказ ФСТЭК России от 22 декабря 2017 г. N 236 7. Приказ ФСТЭК России от 25 декабря 2017 г. N 239 8. Все перечисленные
9	ГОССОПКА это 1. Государственная система по охране окружающей среды 2. Государственная система по разработке полезных ископаемых на холмах и сопках. 3. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы. 4. Государственная система передачи информации об информационных инцидентах.
10	Непредставление или нарушение порядка либо сроков представления в ФСТЭК РФ, сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, предусмотренных законодательством в области обеспечения безопасности КИИ РФ, влечет наложение административного штрафа: 1. На должностных лиц - от десяти тысяч до пятидесяти тысяч рублей; 2. На должностных лиц - от 100 тысяч до пятисот тысяч рублей; 3. На должностных лиц - от одной тысячи до пяти тысяч рублей.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия
Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Критерии значимости объектов критической информационной инфраструктуры подразделяются на 1. Социальная 2. Политическая 3. Экономическая 4. Экологическая 5. Значимость для обеспечения обороны страны, безопасности государства и правопорядка Установите соответствие критерия значимости его содержанию А. Прекращение или нарушение проведения учетно-расчетных операций Б. Причинение ущерба жизни и здоровью людей В. Прекращение или нарушение функционирования государственного органа Г. Снижение показателей государственного оборонного заказа, Д. Вредные воздействия на окружающую среду
12	Установите соответствие систем их назначению 1. DLP; 2. IRP; 3. SIEM; 4. SOC; 5. Deception. А. Централизованная система управления ложными сетевыми объектами, которые принято называть ловушками; Б. Центр мониторинга и реагирования на инциденты информационной безопасности. Специальное подразделение, которое круглосуточно следит за IT-инфраструктурой компании; В. Система управления информационной безопасностью и событиями безопасности. Г. Платформа реагирования на инциденты Д. Система предотвращения утечек информации
13	Объектам критической информационной инфраструктуры (КИИ) присваивают одну из трёх категорий значимости: 1. Первая категория; 2. Вторая категория; 3. Третья категория. Расставьте в соответствии тем последствиям, которые характеризуют данные категории А. Локальные последствия, затрагивающие отдельные подразделения, организации, процессы; Б. Серьёзные последствия на уровне отрасли, региона, крупных экономических потерь; В. Массовые сбои, угроза жизни, национальной безопасности.
14	Существуют 3 категории значимости объектов критической информационной инфраструктуры Российской Федерации и их значений 1 категория 2 категория 3 категория Расставьте в соответствие номеру категории количество человек, которому может быть причинен ущерб по социальной значимости: А. Более 500 Б. Более или равно 1, но менее или равно 50 В. более 50, но менее или равно 500

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Расставьте в порядке значимости нормативные акты, регламентирующие вопросы информационной безопасности: 1. Локальные нормативные акты; 2. Приказы соответствующих Министерств и Ведомств; 3. Законы РФ; 4. Указы Президента РФ; 5. Конституция РФ; 6. Постановления Правительства РФ.
16	Установить правильный порядок действий по категорированию объектов критической информационной инфраструктуры (КИИ) 6. Направление сведений о результатах категорирования в ФСТЭК России; 5. Подготовка акта категорирования объекта КИИ; 4. Категорирование объектов КИИ; 3. Определение перечня объектов КИИ, подлежащих категорированию; 2. Формирование исходных данных для категорирования; 1. Создание комиссии по категорированию.
17	Категорирование объектов КИИ регулируется Федеральным законом №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и Постановлением Правительства РФ №127. Процесс включает несколько этапов: 1. Утверждение и регистрация — результаты категорирования утверждаются в установленном порядке, данные о категорированных объектах заносятся в реестр значимых объектов КИИ РФ. 2. Идентификация объектов — определение информационных систем, сетей и систем управления, которые могут быть отнесены к критическим; 3. Присвоение категории — комиссия присваивает категорию на основе оценки; 4. Оценка значимости — анализ возможных последствий утраты конфиденциальности, целостности или доступности информации; Расставьте эти этапы в правильном порядке

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом

Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Перечислите основные функции ФСТЭК
19	Перечислите сферы, в которых используются объекты критической информационной инфраструктуры (КИИ):
20	Дайте развернутый ответ отличия кибербезопасности от киберзащищенности

Система оценивания выполнения тестовых заданий по компетенции ПК-2, формируемой дисциплиной «ФТД.01 Основы обеспечения безопасности КИИ Российской Федерации»

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 3 баллами. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой; если допущена одна ошибка/неточность/ответ правильный, но не полный - 1 балл, если допущено более одной ошибки/ответ неправильный/ответ отсутствует- 0 баллов.

Ключи к тестовым заданиям по оценке компетенции ПК-2, формируемой дисциплиной «ФТД.01 Основы обеспечения безопасности КИИ Российской Федерации»

№ задания	Верный ответ					
1	3					
2	1					
3	3					
4	1,2,3,4					
5	3					
6	1,2					
7	2					
8	8					
9	3					
10	1					
11	1	2	3	4	5	
	Б	В	А	Д	Г	
12	1	2	3	4	5	
	Д	Г	В	Б	А	
13	1	2	3			
	В	Б	А			
14	1	2	3			
	А	В	Б			
15	5, 3, 4, 6, 2, 1					
16	6,5,4,3, 2, 1					
17	2, 4, 3, 1					
18	К основным функциям ФСТЭК относятся: 1. Обеспечение безопасности критической информационной инфраструктуры 2. Противодействие иностранным техническим разведкам 3. Защита информации 4. Экспортный контроль.					
19	Энергетика; Транспорт. Здравоохранение. Финансы. Связь. Наука. Государственная регистрация прав на недвижимое имущество и сделок с ним. Ракетно-космическая промышленность. Промышленность. Оборона и государственное управление.					
20	Кибербезопасность — это комплекс мер, направленных на защиту компьютерных систем, сетей и данных от несанкционированного доступа, использования, раскрытия, уничтожения или изменения. Киберзащищённость — это свойство объекта инфокоммуникационной среды, характеризующее его возможности предотвращать образование ущерба от кибератак или ограничивать его величину допустимыми нормами.					

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

Перед началом изучения дисциплины преподаватель должен ознакомить обучающихся с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций, преподаватель:

- 1) формулирует тему и цель занятия, объявляет учебные вопросы;
- 2) излагает основные теоретические положения;
- 3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;
- 4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;
- 5) в конце занятия выдает вопросы для самостоятельного изучения.

На занятиях лабораторного цикла следует обратить внимание на соответствие выбираемых обучающимся средств выполнения решаемым в работе задачам.

Каждая лабораторная работа должна быть оформлена и защищена в соответствии с требованиями. Защита производится после оформления отчета по работе.

Во время выполнения заданий в учебной аудитории обучающийся может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, обучающийся может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего контроля и промежуточной аттестации знаний обучающихся.

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, обучающиеся должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы обучающегося на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал

прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности обучающихся.

2.3 Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

- изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д.;
- при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа обучающегося под управлением преподавателя. На них пополняются теоретические знания обучающихся, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение обучающихся к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы.

После подведения итогов занятия обучающийся обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

4. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа обучающихся является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к лабораторным работам (практическим занятиям);
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях.
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов по отдельным вопросам изучаемой дисциплины.

Самостоятельная работа организуется преподавателями, обеспечивается и контролируется кафедрами. Она предусматривает, как правило, разработку рефератов,

выполнение расчетно-графических, вычислительных работ, моделирования и других творческих заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Основная цель данного вида занятий состоит в обучении курсантов методам самостоятельной работы с учебным материалом.

Материал, подлежащий обработке на самостоятельных занятиях, намечается при разработке программы самостоятельной работы. Опыт, накопленный кафедрами в организации самостоятельных занятий, что материал выделяемый на такие занятия, должен удовлетворять следующим требованиям:

- быть изложенным в учебнике достаточно полно и с примерами;
- обеспечиваться достаточным количеством литературы, учебных пособий. учебно-методических материалов, образцов техники
- содержать материал, углубляющий знания, полученные на лекции;
- осваивать проблемные еще не полностью решенные вопросы.

Проведению самостоятельной работы (как и любого другого вида занятий) должна предшествовать подготовка как преподавателя, так и обучаемых.

Постановку задачи обучаемым на проведение самостоятельного занятия преподаватель осуществляет на одном из занятия, предшествующему данному. Он разъясняет смысл занятия и указывает, что к нему обучающиеся должны приготовить. Задание на самостоятельную работу должно быть выдано заблаговременно с тем, чтобы слушатели имели время на информационный поиск в библиотеке необходимых пособий.

Методику самостоятельной работы все обучаемые выбирают индивидуально, но методика достижения конечной цели может определяться преподавателем и включать: последовательность изучения и усвоения учебно-методического материала, пособий, руководств, наставлений, техники и т.д.; определение главного в изучаемом материале, материале, который необходимо законспектировать; просмотр учебных кинофильмов и их обсуждение; работу обучающихся по индивидуальным заданиям; опрос обучаемых в течении 7-10 минут с целью проверки усвоения главного из прочитанного материала.

При возникновении затруднений у обучаемых в разрешении вопросов задания преподавателю необходимо предусмотреть, чтобы каждый обучаемый мог получить оперативную консультацию по любому вопросу, если же при самостоятельной работе возникают затруднения по одному и тому же материалу (вопросу) у многих обучаемых, то желательно провести групповую консультацию.

Для контроля усвоения учебного материала целесообразно проводить в групповое собеседование или обсуждение изучаемого материала, проведение контрольных работ и т.п. Контрольные мероприятия при должной их организации позволяют не только оценивать знания материала, но и углубить и закрепить его у обучаемых.

Приветствуется использование компьютеров, которое:

- расширяет информационную базу учебных занятий;
- повышает активность обучаемых, из пассивного получателя информации они превращаются в её добытчиков:
- способствует развитию способностей к анализу и обобщению, улучшает связанность, широту и глубину мышления;
- облегчает усвоение абстрактного материала, позволяет многое из него представить в виде конкретных образов;
- приучает к точности, аккуратности, последовательности действий способствует развитию самостоятельности.

Компьютерные технологии и программные продукты для выполнения самостоятельной работы по освоению учебного материала необходимо использовать в соответствии с указаниями методических разработок раздела 5 настоящей Рабочей программы.

Таблица – Учебный материал, выносимый на самостоятельное изучение обучающимся очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 18	Неделя
Модуль 1 – 18 часов			
1	Федеральный закон от 26 июля 2017 г. N 187-ФЗ О безопасности критической информационной инфраструктуры Российской Федерации	4	1
2	Постановление Правительства Российской Федерации от 17 февраля 2018 г. N 162 Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации	2	2
3	Приказ ФСТЭК России от 21 декабря 2017 г. N 235 требования к созданию субъектами критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) систем безопасности значимых объектов критической информационной инфраструктуры	2	3
4	Указ Президента Российской Федерации от 5 декабря 2016 г. N 646 инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы	2	4
5	Федеральная служба по техническому и экспортному контролю Информационное сообщение от 17 апреля 2020 г. N 240/84/611 По вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий	2	5
6	Требования по безопасности информации. Утверждены приказом ФСТЭК России от 30 июля 2018 г. N 132 К средствам защиты информации от воздействий, направленных на отказ в обслуживании информационных (автоматизированных) систем Файлы для скачивания: Требования по безопасности информации.	2	6
7	7. Правительство РФ. Постановление от 8 февраля 2018 г. N 127. Об утверждении правил категорирования объектов критической информационной инфраструктуры РФ, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры российской федерации и их значений	4	7

Для более углубленного изучения материала по дисциплине целесообразно использовать учебные курсы сайта <http://www.intuit.ru/>.

Самостоятельная работа обучающихся над усвоением материала по дисциплине может выполняться в помещении для самостоятельной работы СКФ МТУСИ, посредством использования электронной библиотеки и ЭИОС.