МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / А.Ю. Филиппович /
« 28 » мая 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность критической информационной инфраструктуры»
Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль)
«Обеспечение информационной безопасности
распределенных информационных систем»

Квалификация (степень) выпускника
Специалист по защите информации

Форма обучения
Очная
Год приема - 2020

Москва 2020 г.

1. Цели освоения дисциплины

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

- освоение заданных дисциплинарных компетенций в области деятельности по организации и управлению службой защиты информации на критической информационной инфраструктуре, на основе оценки угроз безопасности информации, технологии организации, кадрового, технологического и нормативно-методического обеспечения, политик безопасности, методах оценки эффективности управления системами защиты информации.

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

- изучение методов и средств обеспечения информационной безопасности, механизмов функционирования системы защиты информации на критической информационной инфраструктуре;
- изучение основных принципов и направлений защиты информации на критической информационной инфраструктуре, используемых службой защиты информации;
- установления организационных основ и принципов деятельности службы защиты информации на критической информационной инфраструктуре, определение целей, функций и задач, которые она решает в процессе создания и управления системами организационной зашиты информации.

2. Место дисциплины в структуре ООП

Дисциплина «Безопасность критической информационной инфраструктуры» относится к числу профессиональных учебных дисциплин базовой части цикла (Б.1) основной образовательной программы (Б.1.42).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационной безопасности», «Основы ИКТ», «Криптографические методы защиты информации».

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ПК-6	Способен разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	**знать:** • современные технологии обеспечения информационной безопасности критически важных объектов; • методику проведения аудита

		информационной безопасности на критической информационной инфраструктуре; • порядок организации планирования и контроля работ по безопасности службой защиты информации на критической информационной инфраструктуре. **уметь:** • осуществлять подбор, расстановку кадров и обучение сотрудников службы защиты информации; • организовывать и осуществлять все виды работ службой защиты информации; • организовывать и осуществлять все виды работ службой защиты информации. **владеть:** • методиками оценки эффективности работы службы защиты информации, проведения аудита информационной безопасности на соответствие требованиям безопасности.
ПК-7	Способен участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	**знать:** • методы и средства оптимизации процессов управления критической информационной инфраструктуры (КИИ); • организационно-правовые процессы, регламентирующие создание и использование информационных ресурсов, средств защиты информации, проведение экспертизы, аттестации, сертификации и контроля качества защиты информации и информационных ресурсов критически важных объектов. **уметь:** • применять современные технологии обеспечения информационной безопасности критически важных объектов; • управлять информационной безопасностью критической информационной инфраструктуры (КИИ); • назначение и роль, принципы организации и этапы создания службы защиты информации на предприятии, виды организационных структур службы защиты информации. **владеть:** • методами и средствами проектирования, моделирования и экспериментальной отработки систем, средств и технологий защиты информации на объектах КИИ.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единицы, т.е. **108** академических часов (лабораторные занятия – 72 час, самостоятельная работа - 36 часов, форма контроля – экзамен) в 7 семестре.

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

5. Образовательные технологии

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

- выполнение лабораторных работ в лабораториях вуза;
- индивидуальные и групповые консультации студентов преподавателем, в том числе в виде защиты выполненных заданий в рамках самостоятельной работы;
- посещение профильных конференций и работа на мастер-классах экспертов и специалистов индустрии.

Самостоятельная внеаудиторная работа студентов составляет 50% от общего объема дисциплины и состоит из:

- подготовки к выполнению и подготовки к защите лабораторных работ;
- чтения литературы и освоения дополнительного материала в рамках тематики дисциплины;
- подготовки к текущей аттестации;
- подготовки к промежуточной аттестации.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- экзамен.

Образцы вопросов к экзамену приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать

ПК-6	Способен разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем
ПК-7	Способен участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю):

ПК-6 Способен разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать:	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3)..	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.

уметь:	Обучающийся не умеет или в недостаточной степени умеет выполнять действия, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3).	Обучающийся демонстрирует неполное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности
владеть:	Обучающийся не владеет или в недостаточной степени владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3).	Обучающийся в неполном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Свободно применяет полученные навыки в ситуациях повышенной сложности.

ПК-7 Способен участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**

знать:	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).. .	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.
уметь:	Обучающийся не умеет или в недостаточной степени умеет выполнять действия, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3).	Обучающийся демонстрирует неполное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть:	Обучающийся не владеет или в недостаточной степени владеет приемами, методами и иными умениями, указанными в индикаторах	Обучающийся в неполном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть»	Обучающийся частично владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть»	Обучающийся в полном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины

	компетенций дисциплины «Владеть» (см. п. 3).	(см. п. 3). Допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	(см. п. 3). Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации..	«Владеть» (см. п. 3). Свободно применяет полученные навыки в ситуациях повышенной сложности.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен.

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

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

Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средствпредставлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины

1. Основная литература:

- Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Национальный исследовательский университет – Высшая школа экономики. – Москва : Издательский дом Высшей школы экономики, 2015. – 574 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=440285 (дата обращения: 19.08.2019). – Библиогр. в кн. – ISBN 978-5-7598-0698-1. – Текст : электронный.
- Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – 4-е изд., стер. – Москва : Флинта, 2016. – 224 с. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93351 (дата обращения: 19.08.2019). – Библиогр.: с. 192-193. – ISBN 978-5-9765-1274-0. – Текст : электронный.

2. Дополнительная литература:

- Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 19.08.2019). – Библиогр. в кн. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557. – Текст : электронный.

8. Материально-техническое обеспечение дисциплины

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

Оборудование и аппаратура:

1. Операционная система Microsoft Windows.
2. Веб-браузер Chrome.

9. Методические рекомендации для самостоятельной работы студентов

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

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки **10.05.03 «Информационная безопасность автоматизированных систем»**.

Программу составил: доц. Рагозин Ю.Н.

Программа утверждена на заседании кафедры “Информационная безопасность” «28» мая 2020 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение

**Структура и содержание дисциплины «Безопасность критической информационной инфраструктуры»
по направлению подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
(специалист)**

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
	7 семестр														
1	Определение понятия «Информационная безопасность»; Общая схема обеспечения информационной безопасности.	7	1			4	2								
2	Анализ развития подходов к защите информации; Эмпирический, концептуально-эмпирический и теоретико-концептуальный подходы.		2			4	2								
3	Современная постановка задачи защиты информации; Основные факторы современного этапа; Основные концептуальные положения.		3			4	2								
4	Переход к интенсивным способам		4			4	2								

	защиты информации; Кортеж концептуальных решений; Формирование баз исходных данных.														
5	Определение и принципы формирования теории защиты информации; Общетеоретические принципы формирования теории; Теоретико-прикладные принципы; Методологический базис теории защиты информации.		5			4	2								
6	Методы теории нечетких множеств; Методы теории лингвистических переменных; Неформальные методы оценивания; Неформальные методы поиска оптимальных решений.		6			4	2								
7	Автоформализация знаний эксперта Структура процесса принятия решений; Формирование базы данных; Формирование базы моделей; Принципы построения модели защиты от несанкционированного доступа; Монитор обращений; Правила разграничения доступа; Вербальная модель разграничения доступа; Модель Хартсона; Модель Лэмпсона, Грэхема,		7			4	2								

	Деннинга; Модель Белла и Ла Падула														
8	Обобщенная модель процессов защиты информации; Энтропийный подход к моделированию; Модель системы обеспечения безопасности информации.		8			4	2								
9	Понятие угрозы безопасности информации; Подходы к классификации угроз; Системная классификация угроз; Показатели уязвимости информации Базовый, обобщенный, общий и экстремальные показатели уязвимости; Учет интервала времени оценки.		9			4	2								
10	Оценка достоверности информационной базы прогнозирования показателей уязвимости информации; Модификация фрагментов интегрированной базы данных; Методы обработки свидетельств; Применение методов фильтрации; Алгоритм оптимального фильтра Калмана.		10			4	2								
11	Понятие информационного риска; Модели оценки вероятности проявления угроз безопасности; Модели оценки ущерба от реализации угроз безопасности		11			4	2								

	информации; Динамическая модель оценки потенциальных угроз; Модель оценки ущерба в терминах теории игр; Выводы по рассмотренным моделям.														
12	Постановка задачи определения требований к защите информации; Методики определения требований к защите; Основные действующие документы Российской Федерации; Анализ применяемых методик; Подходы к преодолению недостатков действующих методик; Определение параметров защищаемой информации; Важность информации; Полнота информации; Адекватность информации; Релевантность информации; Толерантность информации; Оценка информации как объекта труда.		12			4	2								
13	Оценка факторов, влияющих на требуемый уровень защиты; Формирование множества факторов; Определение весов и классификация вариантовпотенциально возможных условий защиты информации; Использование методов кластерного анализа;		13			4	2								

	Эмпирический подход к делению на классы.														
14	Определение системы защиты информации; Типизация и стандартизация систем защиты информации; Высший уровень типизации и стандартизации; Средний уровень типизации и стандартизации; Низший уровень типизации и стандартизации; Адаптация и управление развитием систем защиты информации; Многокритериальный развивающийся объект; Монотонный критерий; Формализация политики безопасности; Оценка эффективности процессов защиты.		14			4	2								
15	Общая модель управления системой защиты; Основные макропроцессы управления; Методологические основы выработки управленческих решений; Особенности многокритериальных задач управления;		15			4	2								

	Контроль защищенности информации.														
16	Комплексная политика защиты информации; Функции защиты; Задачи защиты; Средства и методы защиты; Система защиты информации.		16			4	2								
17	Анализ гносеологии развития теории защиты информации; Совершенствование теоретических основ защиты информации; Перевод защиты информации на индустриальную основу; Расширение постановки задачи защиты. Обеспечение информационной безопасности.		17			4	2								
18	Концепция специализированных центров защиты информации; Задачи центров защиты информации; Функции центров защиты информации; Принципы построения центров защиты информации; Автоматизированная сеть центров защиты информации; Формирование баз данных как основная задача центров защиты информации.		18			4	2								
	Форма аттестации	7	19-21							.				Э	
	Всего часов по дисциплине					72	36								

	во седьмом семестре														
	Всего часов по дисциплине					72	36								

Приложение к
рабочей программе

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

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем» ОП (профиль): «Обеспечение информационной безопасности распределенных информационных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая

.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Безопасность критической информационной инфраструктуры»

Состав: 1. Паспорт фонда оценочных средств
2. Описание оценочных средств:
список вопросов к экзамену.

Составители: доц. Рагозин Ю.Н.

Москва, 2020 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Безопасность критической информационной инфраструктуры					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ПК-6	Способен разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	**знать:** • современные технологии обеспечения информационной безопасности критически важных объектов; • методику проведения аудита информационной безопасности на критической информационной инфраструктуре; • порядок организации планирования и контроля работ по безопасности службой защиты информации на критической информационной инфраструктуре. **уметь:** • осуществлять подбор, расстановку кадров и обучение сотрудников службы защиты информации; • организовывать и осуществлять все виды работ службой защиты информации; • организовывать и осуществлять все виды работ службой защиты информации. **владеть:** • методиками оценки эффективности работы службы защиты информации, проведения аудита информационной безопасности на соответствие требованиям безопасности.	самостоятельная работа, лабораторные занятия	экзамен	**Базовый уровень:** **знать:** • методику проведения аудита информационной безопасности на критической информационной инфраструктуре **уметь:** • организовывать и осуществлять все виды работ службой защиты информации **владеть:** • методиками оценки эффективности работы службы защиты информации, проведения аудита информационной безопасности на соответствие требованиям безопасности. **Повышенный уровень:** Знать современные технологии обеспечения информационной безопасности критически важных объектов;методику проведения аудита информационной безопасности на критической информационной инфраструктуре;порядок организации планирования и контроля работ по безопасности службой защиты информации на критической информационной инфраструктуре.Уметь осуществлять подбор, расстановку кадров и обучение сотрудников службы защиты информации;организовывать и осуществлять все виды работ службой защиты информации;организовывать и осуществлять все виды работ службой защиты информации; Владеть методиками оценки эффективности работы службы защиты информации, проведения аудита информационной безопасности на соответствие требованиям безопасности.

ПК-7	Способен участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	**знать:** • методы и средства оптимизации процессов управления критической информационной инфраструктуры (КИИ); • организационно-правовые процессы, регламентирующие создание и использование информационных ресурсов, средств защиты информации, проведение экспертизы, аттестации, сертификации и контроля качества защиты информации и информационных ресурсов критически важных объектов. **уметь:** • применять современные технологии обеспечения информационной безопасности критически важных объектов; • управлять информационной безопасностью критической информационной инфраструктуры (КИИ); • назначение и роль, принципы организации и этапы создания службы защиты информации на предприятии, виды организационных структур службы защиты информации. **владеть:** • методами и средствами проектирования, моделирования и экспериментальной отработки систем, средств и технологий защиты информации на объектах КИИ.	самостоятельная работа, лабораторные занятия	экзамен	**Базовый уровень:** **знать:** • методы и средства оптимизации процессов управления критической информационной инфраструктуры (КИИ) **уметь:** • применять современные технологии обеспечения информационной безопасности критически важных объектов; **владеть:** • методами и средствами проектирования, моделирования и экспериментальной отработки систем, средств и технологий защиты информации на объектах КИИ. **Повышенный уровень:** Знать методы и средства оптимизации процессов управления критической информационной инфраструктуры (КИИ);организационно-правовые процессы, регламентирующие создание и использование информационных ресурсов, средств защиты информации, проведение экспертизы, аттестации, сертификации и контроля качества защиты информации и информационных ресурсов критически важных объектов. Применять современные технологии обеспечения информационной безопасности критически важных объектов;управлять информационной безопасностью критической информационной инфраструктуры (КИИ);назначение и роль, принципы организации и этапы создания службы защиты информации на предприятии, виды организационных структур службы защиты информации. моделирования и экспериментальной отработки систем, средств и технологий защиты информации на объектах КИИ.

Приложение 2
к рабочей программе

Оценочные средства для промежуточной аттестации

Список вопросов для экзамена по дисциплине

1. Определение понятия «Информационная безопасность».
2. Эмпирический, концептуально-эмпирический и теоретико-концептуальный подходы.
3. Определение и принципы формирования теории защиты информации.
4. Теоретико-прикладные принципы.
5. Общетеоретические принципы формирования теории.
6. Методы теории нечетких множеств.
7. Методы теории лингвистических переменных.
8. Неформальные методы оценивания.
9. Неформальные методы поиска оптимальных решений.
10. Принципы построения модели защиты от несанкционированного доступа.
11. Правила разграничения доступа.
12. Понятие угрозы безопасности информации.
13. Подходы к классификации угроз.
14. Системная классификация угроз.
15. Методы обработки свидетельств.
16. Алгоритм оптимального фильтра Калмана.
17. Понятие информационного риска.
18. Модели оценки вероятности проявления угроз безопасности.
19. Модели оценки ущерба от реализации угроз безопасности информации.
20. Методики определения требований к защите.
21. Принципы построения центров защиты информации.
22. Функции центров защиты информации.
23. Задачи центров защиты информации.
24. Комплексная политика защиты информации. Функции защиты. Задачи защиты.
25. Общая модель управления системой защиты.