

ИНСТИТУТ ФИНАНСОВЫХ ТЕХНОЛОГИЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ
КАФЕДРА ФИНАНСОВОГО МОНИТОРИНГА

ОДОБРЕНО УМС ИФТЭБ

Протокол № 545-1

от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки
(специальность)

[1] 10.05.05 Безопасность информационных
технологий в правоохранительной сфере

Семестр	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	В форме практической подготовки/В	СРС, час.	КСР, час.	Форма(ы) контроля, экз./зач./КР/КП
5	5	180	16	16	16		78	0	Э
Итого	5	180	16	16	16	8	78	0	

АННОТАЦИЯ

Дисциплина реализует требования образовательного стандарта НИЯУ МИФИ по направлению подготовки 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» (квалификация (степень) выпускника «специалист»).

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью преподавания дисциплины является изложение студентам номенклатуры, физических принципов работы, структуры, состава, основных характеристик и особенностей применения средств и систем инженерно-технической защиты информации.

Дисциплина относится к числу прикладных дисциплин профессионального цикла дисциплин в силу отбора изучаемого материала и его важности для подготовки специалиста. Курс посвящен изучению теоретических основ средств и систем инженерно-технической защиты информации, рассматриваются номенклатура, физические принципы работы, структура, состав, основные характеристики и особенности применения средств и систем инженерно-технической защиты информации. Подробно анализируются технические средства обнаружения. Рассматриваются вопросы проектирования телевизионных систем наблюдения.

Задачи дисциплины:

- раскрытие содержания базовых понятий инженерно-технической защиты информации;
- изучение номенклатуры, физических принципов работы средств и систем инженерно-технической защиты информации;
- изучение структуры, состава средств и систем инженерно-технической защиты информации;
- изучение основных характеристик и особенностей применения средств и систем инженерно-технической защиты информации.

Таким образом, дисциплина «Инженерно-техническая защита информации» является неотъемлемой составной частью профессиональной подготовки по 090915.65 «Безопасность информационных технологий в правоохранительной сфере». Изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как строгость в суждениях, творческое мышление, организованность и работоспособность, дисциплинированность, самостоятельность и ответственность.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Данная дисциплина является необходимым элементом, обеспечивающим формирование культуры информационной безопасности как необходимого качества любого специалиста, осуществляющего профессиональную деятельность в условиях развития информационного общества. Для успешного освоения дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

- «Математика» (алгебра, геометрия, математический анализ»;
- «Физика»;
- «Информатика и информационные технологии в правоохранительной деятельности»;
- «Философия»;
- «Логика»;
- «Психология».

Знания, полученные при изучении дисциплины «Инженерно-техническая защита информации», используются при изучении дисциплин:

- «Психология воздействия»;
- «Управление информационной безопасностью»;
- «Учебно-исследовательская работа»;
- «Дипломное проектирование».

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-5 [1] – Способен планировать проведение работ по комплексной защите информации на объекте информатизации	3-ОПК-5 [1] – знать основные принципы, правила, процедуры, практические приемы, методы, средства применяемые для обеспечения комплексной защиты информации на объекте информатизации У-ОПК-5 [1] – уметь планировать и проводить работы по комплексной защите информации на объекте информатизации В-ОПК-5 [1] – владеть навыками и стратегиями планирования работ по комплексной защите информации на объекте информатизации
ОПК-6 [1] – Способен применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач	3-ОПК-6 [1] – знать основы теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи У-ОПК-6 [1] – уметь применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач В-ОПК-6 [1] – владеть методами цифровой обработки сигналов, информации и кодирования, электрической связи
ОПК-7 [1] – Способен применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач	3-ОПК-7 [1] – знать основные программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач У-ОПК-7 [1] – уметь применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач В-ОПК-7 [1] – владеть навыками освоения новых программных средств системного и прикладного назначения, языков, методов и инструментальных средств

	программирования для решения профессиональных задач
--	---

Профессиональные компетенции в соответствии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	Объект или область знания	Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)	Код и наименование индикатора достижения профессиональной компетенции
проектно-технологический			
Сбор и анализ исходных данных для проектирования систем обработки и анализа информации с учетом необходимости ее защиты в соответствии с требованиями безопасности информации; участие в проектировании систем, комплексов средств и технологий обработки и защиты информации, в разработке технологической и эксплуатационной документации; адаптация к защищаемым объектам современных информационных технологий и методов обеспечения безопасности информации на основе отечественных и международных стандартов	Информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта); объекты информатизации правоохранительных органов; организационно-правовые механизмы осуществления информационно-аналитической деятельности в правоохранительной сфере; судебно-экспертная деятельность в области компьютерной экспертизы; процессы управления системами, обеспечивающими информационную	ПК-2 [1] - Способен принимать участие в создании системы защиты информации на объекте информатизации <i>Основание:</i> Профессиональный стандарт: 06.033	З-ПК-2[1] - знать основные компоненты системы защиты информации, механизмы создания систем защиты информации, принципы их функционирования ; У-ПК-2[1] - уметь создавать элементы системы защиты информации на объекте информатизации; В-ПК-2[1] - владеть навыками создания системы защиты информации на объекте информатизации

	безопасность на защищаемых объектах, методы и средства оптимизации процессов управления; модели, методы и методики информационно-аналитической деятельности в процессе организационного управления, в том числе, технологии, методы и средства ПОД/ФТ; системы государственного финансового мониторинга; системы финансового мониторинга в кредитных организациях; системы финансового мониторинга в некредитных организациях; системы финансового мониторинга в субъектах первичного финансового мониторинга.		
Установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонент технических систем обеспечения безопасности информации; участие в проведении специальных проверок и исследований, аттестации объектов, помещений, технических средств, систем, сертификационных	эксплуатационный Информационные технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта); объекты информатизации	ПК-3 [1] - Способен организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации <i>Основание:</i> Профессиональный стандарт: 06.032	З-ПК-3[1] - знать основные нормативно-правовые акты и методические документы по обеспечению защиты информации и организационные основы контроля обеспечения защиты информации, в том числе сведений, составляющих государственную тайну, а также методики анализа эффективности систем защиты

испытаний программных средств на предмет соответствия требованиям защиты информации; администрирование подсистем обеспечения информационной безопасности на объекте.	правоохранительных органов; организационно-правовые механизмы осуществления информационно-аналитической деятельности в правоохранительной сфере; судебно-экспертная деятельность в области компьютерной экспертизы; процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления; модели, методы и методики информационно-аналитической деятельности в процессе организационного управления, в том числе, технологии, методы и средства ПОД/ФТ; системы государственного финансового мониторинга; системы финансового мониторинга в кредитных организациях; системы финансового мониторинга в некредитных организациях; системы финансового мониторинга в субъектах первичного финансового мониторинга.		информации ; У-ПК-3[1] - уметь организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации; В-ПК-3[1] - владеть навыками организации и проведения мероприятий по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, а также проведения анализа эффективности системы защиты информации
Установка,	Информационные	ПК-4 [1] - Способен	3-ПК-4[1] - знать

настройка, эксплуатация и поддержание в работоспособном состоянии компонент технических систем обеспечения безопасности информации; участие в проведении специальных проверок и исследований, аттестации объектов, помещений, технических средств, систем, сертификационных испытаний программных средств на предмет соответствия требованиям защиты информации; администрирование подсистем обеспечения информационной безопасности на объекте.	технологии и системы, а также информационные процессы и ресурсы в правоохранительной деятельности; технологии защиты информации и информационных ресурсов, обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта); объекты информатизации правоохранительных органов; организационно-правовые механизмы осуществления информационно-аналитической деятельности в правоохранительной сфере; судебно-экспертная деятельность в области компьютерной экспертизы; процессы управления системами, обеспечивающими информационную безопасность на защищаемых объектах, методы и средства оптимизации процессов управления; модели, методы и методики информационно-аналитической деятельности в процессе организационного управления, в том числе, технологии, методы и средства	способностью участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации <i>Основание:</i> Профессиональный стандарт: 06.034	основные нормативно-правовые акты и методические документы, содержащие требования к аттестационным испытаниям и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации, а также методы и методологию их проведения ; У-ПК-4[1] - уметь осуществлять аттестационные испытания и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации; В-ПК-4[1] - владеть навыками участия в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации
---	--	---	---

	ПОД/ФТ; системы государственного финансового мониторинга; системы финансового мониторинга в кредитных организациях; системы финансового мониторинга в некредитных организациях; системы финансового мониторинга в субъектах первичного финансового мониторинга.		
--	---	--	--

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих, формирование научного мировоззрения, культуры поиска нестандартных научно-технических/практических решений, критического отношения к исследованиям лженаучного толка (В19)	1.Использование воспитательного потенциала дисциплин/практик «Научно-исследовательская работа», «Проектная практика», «Научный семинар» для: - формирования понимания основных принципов и способов научного познания мира, развития исследовательских качеств студентов посредством их вовлечения в исследовательские проекты по областям научных исследований. 2.Использование воспитательного потенциала дисциплин "История науки и инженерии", "Критическое мышление и основы научной коммуникации", "Введение в специальность", "Научно-исследовательская работа", "Научный семинар" для: - формирования способности отделять настоящие научные исследования от лженаучных посредством проведения со студентами занятий и регулярных бесед; - формирования критического мышления, умения рассматривать различные исследования с

		экспертной позиции посредством обсуждения со студентами современных исследований, исторических предпосылок появления тех или иных открытий и теорий.
Профессиональное воспитание	Создание условий, обеспечивающих, формирование культуры информационной безопасности (В23)	Использование воспитательного потенциала дисциплин профессионального модуля для формирования базовых навыков информационной безопасности через изучение последствий халатного отношения к работе с информационными системами, базами данных (включая персональные данные), приемах и методах злоумышленников, потенциальном уроне пользователям.

5. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практи. (семинары) / Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	<i>5 Семестр</i>						
1	Раздел 1	1-5	8/8/8	к.р-8	25	КИ-8	
2	Раздел 2	6-16	8/8/8	к.р-15	25	КИ-15	
	<i>Итого за 5 Семестр</i>		16/16/16		50		
	Контрольные мероприятия за 5 Семестр				50	Э	

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	Полное наименование
КИ	Контроль по итогам

к.р	Контрольная работа
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недел и	Темы занятий / Содержание	Лек., час.	Пр./сем. , час.	Лаб., час.
	<i>5 Семестр</i>	16	16	16
1-5	Раздел 1	8	8	8
1	Тема 1. Введение. Основные понятия и определения. Основные понятия и определения. Система безопасности, стратегия безопасности, обеспечение безопасности объектов охраны. Виды и типы безопасности. Факторы обеспечения безопасности. Концепция комплексного обеспечения безопасности объектов охраны.	Всего аудиторных часов		
		1	1	1
		Онлайн		
2	Тема 2. Технические системы охраны и физической защиты объектов. Технические системы охраны и физической защиты объектов. Определение целей, задач, назначение технических систем охраны и физической защиты. Технические средства охраны. Нормативные документы по техническим средствам и системам охраны (системам физической защиты) объектов.	Всего аудиторных часов		
		1	1	1
		Онлайн		
3	Тема 3. Угрозы. Виды и типы угроз. Угрозы. Виды и типы угроз. Порядок определения угроз. Потенциальные (возможные) угрозы, модель нарушителя. Классификация нарушителей, вероятные пути и методы проникновения. Выявление целей нарушителей, предметов защиты (уязвимых мест). Оценка возможного ущерба от реализации прогнозируемых угроз.	Всего аудиторных часов		
		1	1	1
		Онлайн		
4	Тема 4. Порядок проведения обследования объектов охраны. Порядок проведения обследования объектов охраны. Определение характеристик объекта охраны. Физические (физико-географические, метеорологические, климатические) условия места размещения объекта. Инфраструктура места размещения объекта. Режимы, правила, условия, регламентирующие функционирование объекта. Организация охраны объекта.	Всего аудиторных часов		
		1	1	1
		Онлайн		
5	Тема 5. Оценка уровня уязвимости объекта охраны. Оценка уровня уязвимости объекта охраны. Категорирование объектов охраны, цель и задачи, основные подходы. Факторы, влияющие на категорирование объектов.	Всего аудиторных часов		
		1	1	1
		Онлайн		
6	Тема 6. Технические средства обнаружения. Технические средства обнаружения. Основы построения. Устройство и принцип действия. Классификация.	Всего аудиторных часов		
		1	1	1
		Онлайн		
7	Тема 7. Основные характеристики качества технических средств обнаружения.	Всего аудиторных часов		
		1	1	1

	Основные характеристики качества технических средств обнаружения. Алгоритмы функционирования технических средств обнаружения.	Онлайн		
8	Тема 8. Датчики охранной сигнализации. Датчики охранной сигнализации. Классификация. Принципы работы датчиков. Факторы, влияющие на работу датчиков.	Всего аудиторных часов		
		1	1	1
		Онлайн		
6-16	Раздел 2	8	8	8
9	Тема 9. Система сбора и обработки информации (ССОИ). Система сбора и обработки информации. Введение. ССОИ аппаратно-программная система обеспечения взаимодействия человека с КТСО. Классификация ССОИ.	Всего аудиторных часов		
		1	1	1
		Онлайн		
10	Тема 10. Система контроля и управления доступом. Особенности построения систем контроля доступа. Функциональные возможности систем контроля доступа. Периферийное оборудование и носители информации систем контроля доступа. Средства идентификации и аутентификации. Рекомендации по выбору средств и систем контроля доступа.	Всего аудиторных часов		
		1	1	1
		Онлайн		
11 - 12	Тема 11. Телевизионные системы наблюдения. Тема 12. Вопросы проектирования телевизионных систем наблюдения. Назначение, состав и общие требования к телевизионным системам охранного наблюдения. Телевизионные камеры и устройства для их оснащения. Объективы. Видеоомониторы. Делители экрана (квадраторы). Видеомультиплексоры. Видеозапись. Общие положения. Организация проектирования. Перечень основных вопросов, уточняемых при проектировании. Выбор и размещение оборудования.	Всего аудиторных часов		
		2	2	2
		Онлайн		
13	Тема 13. Инженерно-технические средства физической защиты. Принципы устройства и типы инженерных заграждений. Требования к инженерно-техническим средствам физической защиты.	Всего аудиторных часов		
		1	1	1
		Онлайн		
14	Тема 14. Обеспечивающие системы, сооружения, транспортные и регламентные средства. Системы электроснабжения. Общие сведения. Потребители электроэнергии в технических системах охраны и физической системы защиты. Особенности принципов построения аппаратуры электропитания. Автономные источники питания. Системы: тепло-, воздухо-, водоснабжения, пожаротушения, охранного освещения, оперативной связи и т.д. Специальные сооружения: помещения подразделений (служб) охраны объекта, караульное помещение, КПП, наблюдательные вышки часовых и др. Транспортные (специальные транспортные) средства.	Всего аудиторных часов		
		1	1	1
		Онлайн		
15 - 16	Тема 15. Основные характеристики качества технических систем охраны и физической защиты и методические положения об их оценке на этапах	Всего аудиторных часов		
		2	2	2
		Онлайн		

	проектирования и испытаний. Основные характеристики технических систем охраны и физической защиты объектов: эффективность; устойчивость функционирования; надежность; живучесть и стойкость к внешним воздействиям; безопасность эксплуатации; стоимость.			
--	---	--	--	--

Сокращенные наименования онлайн опций:

Обозначение	Полное наименование
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ЛАБОРАТОРНЫХ РАБОТ

Недели	Темы занятий / Содержание
	<i>5 Семестр</i>
1 - 2	Лабораторная работа № Введите здесь подробное описание пункта
3 - 4	Лабораторная работа № Введите здесь подробное описание пункта
5 - 6	Лабораторная работа № Введите здесь подробное описание пункта
7 - 8	Лабораторная работа № Введите здесь подробное описание пункта
9 - 10	Лабораторная работа № Введите здесь подробное описание пункта
11 - 12	Лабораторная работа № Введите здесь подробное описание пункта
13 - 14	Лабораторная работа № Введите здесь подробное описание пункта
15 - 16	Лабораторная работа № Введите здесь подробное описание пункта

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	Темы занятий / Содержание
	<i>5 Семестр</i>
1	Тема 1. Введение. Основные понятия и определения. Основные понятия и определения. Система безопасности, стратегия безопасности, обеспечение безопасности объектов охраны.
2	Тема 2. Технические средства охраны.

	Технические средства охраны. Нормативные документы по техническим средствам и системам охраны (системам физической защиты) объектов.
3	Тема 3. Угрозы. Угрозы. Виды и типы угроз.
4	Тема 4. Порядок проведения обследования объектов охраны Порядок проведения обследования объектов охраны
5	Тема 5. Оценка уровня уязвимости объекта охраны. Оценка уровня уязвимости объекта охраны.
6	Тема 6. Технические средства обнаружения. Технические средства обнаружения. Основы построения. Устройство и принцип действия. Контрольная работа №1.
7	Тема 7. Основные характеристики качества технических средств обнаружения. Основные характеристики качества технических средств обнаружения.
8	Тема 8. Датчики охранной сигнализации. Датчики охранной сигнализации.
9	Тема 9. Система сбора и обработки информации (ССОИ). Система сбора и обработки информации (ССОИ).
10	Тема 10. Система контроля и управления доступом. Система контроля и управления доступом
11 - 12	Темы 11-12. Телевизионные системы наблюдения Назначение, состав и общие требования к телевизионным системам охранного наблюдения. Телевизионные камеры и устройства для их оснащения. Объективы. Видеомониторы. Дели-тели экрана (квадраторы). Видеомуль-типлексоры. Видеозапись.
13	Тема 13. Организация проектирования телевизионных систем наблюдения. Организация проектирования телевизионных систем наблюдения.
14	Тема 14. Принципы устройства и типы инженерных заграждений. Принципы устройства и типы инженерных заграждений.
15	Тема 15. Обеспечивающие системы, сооружения, транспортные и регламентные средства. Обеспечивающие системы, сооружения, транспортные и регламентные средства. Контрольная работа №2
16	Тема 16. Основные характеристики качества технических систем охраны. Основные характеристики качества технических систем охраны

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Дисциплина сформирована как курс лекций, при чтении которых используются современные мультимедийные средства и семинарские занятия, при проведении которых используются современные мультимедийные средства. Для самостоятельной работы студентов используется подготовленный конспект лекций и рекомендуемая преподавателем учебная литература (основная и дополнительная), указанные в рабочей программе учебной дисциплины «Инженерно-техническая защита информации».

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	Индикаторы освоения
-------------	---------------------

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – <i>«отлично»</i>	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – <i>«хорошо»</i>	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69	3 – <i>«удовлетворительно»</i>	E	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64			
Ниже 60	2 –	F	Оценка «неудовлетворительно»

	«неудовлетворительно»		выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.
--	-----------------------	--	--

Оценочные средства приведены в Приложении.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. 65 М82 Изучение универсального метода проектирования систем инженерно-технической защиты объектов : учебное пособие, А. С. Мосолов, Е. А. Беляева, А. В. Бадиков, Москва: НИЯУ МИФИ, 2010
2. ЭИ М82 Изучение универсального метода проектирования систем инженерно-технической защиты объектов : учебное пособие для вузов, А. С. Мосолов, Е. А. Беляева, А. В. Бадиков, Москва: НИЯУ МИФИ, 2010
3. 004 М48 Информационная безопасность и защита информации : Учебное пособие для вузов, В. П. Мельников , С. А. Клейменов , А. М. Петраков , Москва: Академия, 2009

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 654 Ш46 Охрана объектов. Техника и технологии : учебное пособие для вузов, Москва: Энергоатомиздат, 2005
2. 004 Т61 Инженерно-техническая защита информации : учеб. пособие для вузов, А. А. Торокин, М.: Гелиос АРВ, 2005
3. 621.039 С59 Средства и системы охранной сигнализации : учебно-методическое пособие, Е. Е. Соколов, Москва: МИФИ, 2006

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

<https://online.mephi.ru/>

<http://library.mephi.ru/>

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Текущий контроль качества усвоения учебного материала по дисциплине.

Для получения положительной оценки необходимо освоить основные теоретические положения дисциплины и уметь разрабатывать и представлять презентацию по материалу курса. В процессе изучения предмета в течение учебного семестра необходимо написать на положительные оценки 2 контрольные работы, содержащие типовые вопросы по материалу курса.

Итоговая аттестация по дисциплине.

Изучение курса завершается зачетом (максимальный балл - 50).

Необходимым условием успешного завершения курса является твердое знание следующих основных понятий, положений и методик:

система безопасности, стратегия безопасности, обеспечение безопасности объектов охраны;

технические системы охраны и физической защиты объектов;

угрозы, виды и типы угроз, порядок определения угроз, потенциальные (возможные) угрозы, модель нарушителя;

порядок проведения обследования объектов охраны;

оценка уровня уязвимости объекта охраны;

технические средства обнаружения;

основные характеристики качества технических средств обнаружения;

принципы работы датчиков охранной сигнализации;

система сбора и обработки информации;

система контроля и управления доступом;

назначение, состав и общие требования к телевизионным системам охранного наблюдения;

особенности проектирования телевизионных систем наблюдения;

принципы устройства и типы инженерных заграждений;

обеспечивающие системы, сооружения, транспортные и регламентные средства;

основные характеристики технических систем охраны и физической защиты объектов: эффективность; устойчивость функционирования; надежность; живучесть и стойкость к внешним воздействиям; безопасность эксплуатации; стоимость.

Автор(ы):

Модестов Алексей Альбертович

