МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

ИНТЕГРИРОВАННЫЕ СИСТЕМЫ ОХРАНЫ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) подготовки:
Безопасность автоматизированных систем
Уровень квалификации выпускника – бакалавр

Форма обучения очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Интегрированные системы охраны
Рабочая программа дисциплины
Составитель:
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№_10_ от__20.05.2021 г._____

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины:

Цель дисциплины – профессиональная подготовка студентов, необходимая для освоения методов и технологий, связанных с обеспечением безопасности объекта информатизации от физического доступа посторонних лиц.

Задачи дисциплины:
– получение систематизированных знаний о современных концепциях, методах и технологиях обеспечения безопасности объекта информатизации от физического доступа посторонних лиц;
–• формирование умений использовать современные достижения в области обеспечения безопасности объекта информатизации от физического доступа посторонних лиц при реализации своей профессиональной деятельности;
– владение практическими навыками, применения современных методами, сил и средств в обеспечении безопасности объекта информатизации от физического доступа посторонних лиц;
– развитие аналитического мышления, умения строго излагать свои мысли, развитие способностей к обобщению и анализу информации, постановке целей и выбору путей ее достижения.

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-3 Способен управлять защитой информации в автоматизированных системах	*ПК-3.1 Знает основные методы управления защитой информации, информационные ресурсы автоматизированных систем, подлежащие защите; основные угрозы безопасности информации, модели нарушителя в автоматизированных системах*	*Знать:* • *модели нарушителя объекта охраны, на котором размещена АС.*
	ПК-3.2 Умеет разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; классифицировать и оценивать угрозы безопасности информации; оценивать информационные риски в автоматизированных системах	*Уметь:* • *организовать работу по обеспечению безопасности объектов охраны от воздействия источников угроз и реализации угроз.*
	ПК-3.3 Владеет навыками составления комплекса правил, процедур, практических приёмов, принципов и методов, средств	*Владеть:* • *практическими навыками по использованию нормативных и руководящих документов в*

	обеспечения защиты информации в автоматизированной системе	*организации работ по защите объектов охраны*
ПК-7 *Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений*	*ПК-7.1* *Знает разработку концепции средств и систем информатизации в защищённом исполнении, разработку технического задания на средство и/или систему информатизации в защищённом исполнении*	*Знать:* • *состав и порядок разработки нормативных документов по обеспечению безопасности объектов охраны.* • *состав, структуру и принципы работы интегрированных систем охраны и их элементов*
	ПК-7.2 *Умеет разрабатывать конструкторскую и технологическую документацию на средство и/или систему информатизации в защищённом исполнении*	*Уметь:* • *выбирать технические средства охраны, системы контроля и управления доступом, системы видеонаблюдения для выполнения профессиональных задач.*
	ПК-7.3 *Владеет навыками разработки рабочей и эксплуатационной документации на средства и системы информатизации в защищённом исполнении*	*Владеть:* • *навыками проектирования интегрированных систем охраны;* • *навыками безопасного использования технических средств в профессиональной деятельности.*
ПК-10 *Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности*	*ПК-10.1* *Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации*	*Знать:* • *требования нормативных и руководящих документов РФ по обеспечению безопасности объектов охраны.*
	ПК-10.2 *Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации*	*Уметь:* • *разрабатывать нормативные документы по обеспечению безопасности объектов охраны, на которых размещена АС, от физического доступа посторонних лиц.*

	ПК-10.3 *Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации*	*Владеть:* • *навыками по моделированию источников угроз и угроз безопасности объектов охраны, на которых размещена АС.*

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Интегрированные системы охраны» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Основы информационной безопасности», «Электротехника», «Электроника и схемотехника»

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Методы и средства защиты информации от утечки по техническим каналам», «Биометрические системы аутентификации», «Аттестация объектов информатизации».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет _2_ з.е., _76__ ч., в том числе контактная работа обучающихся с преподавателем _40_ ч., промежуточная аттестация _-_ ч., самостоятельная работа обучающихся _36_ ч.

№ п/п	Темы дисциплины/	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1.	*Основные положения по защите объекта охраны*	**5**	**2**	–	–	–	–	**2**	
2.	*Факторы, влияющие на состояние защищённости объекта охраны, классификация нарушителя*	**5**	**2**	–	–	–	–	**2**	Устный опрос.
3.	*Классификация интегрированных систем охраны*	**5**	**2**	–	–	–	–	**2**	Устный опрос.
4.	*Инженерные средства охраны*	**5**	**2**		–	–	–	**2**	Устный опрос.
5.	*Системы контроля и управления доступом*		**2**					**2**	
6.	*Охранно-пожарные извещатели*	**5**	**2**		–	–	–	**2**	Устный опрос.
7.	*Охранное телевидение и видеонаблюдение*	**5**	**2**		–	–	–	**2**	Устный опрос.
8.	*Методические рекомендации по построению системы защиты объекта охраны*	**5**	**2**		–	–	–	**2**	Устный опрос.
10.	*Практическая работа № 1*	**5**	–	–	**6**		–	**4**	Выполнение и защита практической работы.
11.	*Практическая работа № 2*	**5**	–	–	**8**	–	–	**6**	Выполнение и защита практической работы.
12.	*Практическая работа № 3*	**5**	–	–	**8**	–	–	**6**	Выполнение и защита практической работы.
.	*зачёт*	**5**	–	–	**2**	–	–	**4**	Зачёт по билетам
	Итого:		**16**		**24**			**36**	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	***Тема 1. Основные положения по защите объекта охраны***	Термины и определения, основные нормативные и правовые документы по интегрированным системам охраны (ИСО). Основные положения системного подхода к ИСО. Понятие системного подхода, основные методы при моделировании системы защиты информации, сущность системного подхода. Понятие системы защиты объектов охраны от физического доступа, цели, задачи, принципы построения, основные показатели. Многозональность пространства, многорубежность, равнопрочность рубежей системы охраны объектов, скрытность и надёжность технических средств охраны.
2	***Тема 2. Факторы, влияющие на состояние защищённости объекта охраны, классификация нарушителя***	Объект защиты, классификация и категорирование объекта защиты. Факторы, влияющие на обеспечение безопасности объектов охраны от воздействия источников угроз и исключение или минимизация случаев реализации угроз. Факторы обеспечения безопасности объекта защиты от физического доступа посторонних лиц, несанкционированного вноса/выноса материальных и финансовых средств, носителей сведений конфиденциального характера, перечень субъективных и объективных факторов, которые влияют на эффективность защиты информации (такие как время реакции, задержки и нейтрализации источников угроз.). Модель поведения нарушителя.
3	***Тема 3. Классификация интегрированных систем охраны***	Структура интегрированных систем охраны. Системы контроля и управления доступом. Технические средства охраны. Технические средства обнаружения угрозы, средства отражения угрозы и средства ликвидации (нейтрализации) угрозы, назначение и решаемые задачи. Основные положения по повышению надёжности и отказоустойчивости интегрированных систем охраны. Меры по повышению вероятности обнаружения источника угроз и исключения ложного срабатывания технических средств охраны. Управление силами и средствами системы охраны объекта. Цели, задачи, принципы и основные выполняемые функции. Показатели

		эффективности системы управления силами и средствами по охране объекта.
4	***Тема 4. Инженерные средства охраны***	Классификация и назначение инженерных средства охраны объектов. Классификация и особенности ограждений периметра. Назначение и основные требования к естественным и искусственным преградам. Организация инженерной защиты зданий. Освещение рубежей и контролируемых зон. Предъявляемые требования к коммуникациям и другим технологическим каналам, находящиеся на охраняемой территории.
5	***Тема 5. Системы контроля и управления доступом***	Классификация, назначение системы контроля и управления доступом (СКУД) в системе обеспечения безопасности объектов охраны. Структура и основные технические компоненты СКУД. Типовые варианты СКУД. Идентификаторы пользователя. Назначение идентификаторов пользователя. Виды, принцип работы, технические характеристики. Считыватели для электронных идентификаторов. Виды считывателей. Способы ввода считывания идентификационных признаков. Состав и назначение технических элементов контроллера. Технические параметры контроллера. Комбинированные контроллеры выполняемые функции при наличии и отсутствии. связи или выхода из строя управляющего компьютера. Исполнительные устройства СКУД. Виды и принцип работы исполнительных устройств. раны.
6	***Тема 6. Охранно-пожарные извещатели***	Классификация технических средств обнаружения. Назначение, задачи состав, технические характеристики извещателей. Классификация извещателей по принципу работы, применения, обнаружения. Требования к оборудованию внешних рубежей охраны. Виды периметровых средств обнаружения. Методика определения варианта оборудования объектов техническими средствами охраны. Выбор средств сбора и обработки информации. Классификация пожарных извещателей.
7	***Тема 7. Охранное телевидение и видеонаблюдение***	Способы и средства видеоконтроля. Структура системы видеоконтроля. Назначение, состав и классификация

		телевизионных систем наблюдения. Телевизионные камеры и мониторы. Выбор средств видеонаблюдения для оборудования объекта..
8	***Тема 8. Методические рекомендации по построению системы защиты объектов охраны***	Понятие о моделировании как основном процессе системного анализа при исследовании проблем охраны объекта защиты. Моделирование объекта защиты, возможных методов и способов обхода и взлома ИСО. Методические рекомендации по разработке системы безопасности объекта с использованием типовых технических решений, требований нормативных и руководящих документов по обеспечению безопасности объектов охраны. Способы оценки состояния безопасности объекта охраны и величина расходов на построение и эксплуатацию ИТСО. Оценка эффективности системы безопасности объекта охраны от физического доступа посторонних лиц.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	Основные положения по защите объекта охраны	Лекция 1. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
2	Факторы, влияющие на состояние защищённости объекта охраны, классификация нарушителя	Лекция 2. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
3	Классификация интегрированных систем охраны	Лекция 3. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
4	Инженерные средства охраны	Лекция 4. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
5	Системы контроля и управления доступом	Лекция 5. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
6	Охранно-пожарные извещатели	Лекция 6. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
7	Охранное телевидение и видеонаблюдение	Лекция 7. Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
8	Методические рекомендации по построению системы защиты объекта охраны	Лекция 8 Самостоятельная работа	Традиционная с использованием презентаций. Изучение материала по теме.
9	Практическая работа № 1	Практическая работа Самостоятельная работа	Выполнение и защита практической работы.
10	Практическая работа № 2	Практическая работа Самостоятельная работа	Выполнение и защита практической работы.
11	Практическая работа № 3	Практическая работа Самостоятельная работа	Выполнение и защита практической работы.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
- опрос (темы 1-8) - практическое занятие (1-3)	3 12	24 36
Промежуточная аттестация зачёт		40 баллов
Итого за семестр зачёт		100 баллов

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	***Контролируемые разделы (темы) дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	*Тема 1.*	ПК-3.1, ПК-3.2, ПК-7.1, ПК-7.2	Опрос
2.	*Тема 2.*	ПК-3.1, ПК-3.2, ПК-3.3, ПК-10.1, ПК-10.2, ПК-10.3	Опрос
3.	*Тема 3.*	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,	Опрос
4.	*Тема 4.*	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,	Опрос
5.	*Тема 5.*	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,	Опрос
6.	*Тема 6.*	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,	Опрос
7.	*Тема 7.*	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,	Опрос
8.	*Тема 8.*	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,	Опрос
10.	*Практическая работа № 1, 2, 3*	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,	План практического занятия

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A, B	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D, E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
49-0/ F,FX	«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний обучающегося по определённому разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

№	Вопрос	Реализуемая компетенция
1.	Основные положения системного и комплексного подхода к построению системы охраны объекта защиты?	ПК-3.1, ПК-3.2, ПК-7.1, ПК-7.2
2.	Цели, задачи и принципы построения системы охраны объекта защиты.	ПК-3.1, ПК-3.2, ПК-7.1, ПК-7.2
3.	Модель поведения внешнего нарушителя на этапах реализации угроз безопасности информации, методы и способы противодействия.	ПК-3.1, ПК-10.1
4.	Модель поведения внутреннего нарушителя на этапах реализации угроз безопасности информации, методы и способы противодействия.	ПК-3.1, ПК-10.1
5.	Модель поведения нарушителя при использовании технических средств взлома, обхода ИСО.	ПК-3.1, ПК-10.1
6.	Какие условия и факторы, способствующие несанкционированному проникновению на объект защиты, методы и способы противодействия несанкционированному проникновению?	ПК-3.1, ПК-3.2, ПК-3.3, ПК-10.1, ПК-10.2, ПК-10.3,
7.	Назначение технических средств охраны в системе обеспечения безопасности объектов от физического доступа посторонних лиц.	ПК-3.1, ПК-10.1,
8.	Виды СКУД	ПК-7.1, ПК-7.2, ПК-7.3
9.	Виды электронных идентификаторов	ПК-7.1, ПК-7.2, ПК-7.3
10.	Виды биометрических идентификаторов	ПК-7.1, ПК-7.2, ПК-7.3
11.	Виды считывателей	ПК-7.1, ПК-7.2, ПК-7.3

12.	Основные понятия и классификация источников угроз, угроз безопасности объектов защиты, степень нанесения ущерба в зависимости от реализации угроз.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-10.1, ПК-10.2, ПК-10.3,
13.	Назначение, основные задачи системы охранного видеонаблюдения.	ПК-7.1, ПК-7.2, ПК-7.3
14.	Состав и технические характеристики системы и отдельных элементов системы охранного видеонаблюдения.	ПК-7.1, ПК-7.2, ПК-7.3
15.	Видеоконтроль – как основной способ контроля доступа на объект охраны (в помещение).	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
16.	Организация общей системы видеоконтроля.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
17.	Обработка и хранение видеозаписей.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
18.	Структура системы охранного видеонаблюдения..	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
19.	Способы передачи видеосигнала по общим каналам связи.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
20.	Типовые схемы телевизионных систем контроля и наблюдения.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
21.	Требования при лицензировании и сертификации деятельности охранной организации по обеспечению безопасности объекта защиты.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-10.1, ПК-10.2, ПК-10.3,
22.	Какие нормативно-правовые документы, необходимые для разработки и эксплуатации системы обеспечения безопасности объекта от физического доступа посторонних лиц?	ПК-3.1, ПК-3.2, ПК-3.3, ПК-10.1, ПК-10.2, ПК-10.3,
23.	Какие модели используются при построении системы защиты объекта, переход от практического опыта к концептуальной научно-технической модели при разработке системы безопасности объекта охраны?	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
24.	Категорирование объектов охраны по важности (ценности) объекта охраны и по возможным способам несанкционированного доступа.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-10.1, ПК-10.2, ПК-10.3,
25.	Назовите основные требования для охраны важных помещений (помещения группы Б).	ПК-3.1, ПК-3.2, ПК-3.3, ПК-10.1, ПК-10.2, ПК-10.3,
26.	Назовите основные требования для охраны особо важных помещений (помещения группы А).	ПК-3.1, ПК-3.2, ПК-3.3, ПК-10.1, ПК-10.2, ПК-10.3,
27.	Организационные методы контроля эффективности защиты информации на примере вербального объекта.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-10.1, ПК-10.2, ПК-10.3,
28.	Технические методы контроля эффективности защиты информации на примере вербального объекта.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-10.1, ПК-10.2, ПК-10.3,

Промежуточная аттестация (зачёт) – проверка сформированности компетенций – ПК-3, ПК-7, ПК-10

№	Вопрос	Реализуемая компетенция

1.	Основные положения концепции технической защиты информации. Системный подход при построении системы защиты информации. Цели и задачи системы защиты объекта охраны.	ПК-3.1, ПК-3.2, ПК-7.1, ПК-7.2
2.	Цели, задачи и принципы технической защиты объекта охраны.	ПК-3.1, ПК-3.2, ПК-7.1, ПК-7.2
3.	Особенности охраны объекта защиты в системе обеспечения безопасности информации. Назначение и характеристики технических средств охраны и видеонаблюдения.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
4.	Факторы обеспечения защиты материальных ценностей и носителей информации от угроз воздействия.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-10.1, ПК-10.2, ПК-10.3,
5.	Источники угроз, угрозы безопасности объекта, модель поведения нарушителя при несанкционированном проходе на объект защиты.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
6.	Классификация методов и способов охраны объекта. Структура системы обеспечения безопасности объекта от физического доступа посторонних лиц.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
7.	Структура, цели и задачи системы безопасности объекта охраны от физического доступа.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
8.	Современная концепция защиты объектов от физического доступа посторонних лиц.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
9.	Виды систем охраны объекта. Система автономной охраны. Система централизованной охраны.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
10.	Использование физических свойств нарушителя в практике обоснованного применения технических средств охраны.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
11.	Классификация извещателей по назначению, виду и принципу обнаружения и т.п.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
12.	Назначение, состав, принцип работы, технические характеристики контактных извещателей.	ПК-7.1, ПК-7.2, ПК-7.3
13.	Назначение, состав, технические характеристики принцип работы омических извещателей.	ПК-7.1, ПК-7.2, ПК-7.3
14.	Назначение, состав, технические характеристики, принцип работы вибрационных извещателей.	ПК-7.1, ПК-7.2, ПК-7.3
15.	Назначение, состав, технические характеристики, принцип работы оптико-электронных извещателей.	ПК-7.1, ПК-7.2, ПК-7.3
16.	Назначение, состав, технические характеристики, принцип работы радиоволновых извещателей.	ПК-7.1, ПК-7.2, ПК-7.3
17.	Назначение, состав, технические характеристики, принцип работы ультразвуковых извещателей.	ПК-7.1, ПК-7.2, ПК-7.3
18.	Назначение, состав, технические характеристики, принцип работы емкостных извещателей.	ПК-7.1, ПК-7.2, ПК-7.3
19.	Назначение, состав, технические характеристики, принцип работы комбинированных извещателей.	ПК-7.1, ПК-7.2, ПК-7.3
20.	Классификация, назначение СКУД в системе обеспечения безопасности объектов охраны.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3,

		ПК-10.1, ПК-10.2, ПК-10.3,
21.	Структура и основные технические компоненты СКУД.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
22.	Типовые варианты СКУД.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
23.	Идентификаторы пользователя. Назначение идентификаторов пользователя. Виды, принцип работы, технические характеристики.	ПК-7.1, ПК-7.2, ПК-7.3
24.	Считыватели для электронных идентификаторов. Виды считывателей. Способы ввода считывания идентификационных признаков.	ПК-7.1, ПК-7.2, ПК-7.3
25.	Состав и назначение технических элементов контроллера. Технические параметры контроллера.	ПК-7.1, ПК-7.2, ПК-7.3
26.	Комбинированные контроллеры выполняемые функции при наличии и отсутствии. связи или выхода из строя управляющего компьютера.	ПК-7.1, ПК-7.2, ПК-7.3
27.	Исполнительные устройства СКУД. Виды и принцип работы исполнительных устройств.	ПК-7.1, ПК-7.2, ПК-7.3
28.	Требования к оборудованию внутренних рубежей охраны.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
29.	Требования к оборудованию внешних рубежей охраны.	ПК-7.1, ПК-7.2, ПК-7.3
30.	Виды периметровых средств обнаружения.	ПК-7.1, ПК-7.2, ПК-7.3
31.	Радиолучевые средства обнаружения, назначение, состав, технические характеристики, принцип работы.	ПК-7.1, ПК-7.2, ПК-7.3
32.	Радиотехнические средства обнаружения, назначение, состав, технические характеристики, принцип работы.	ПК-7.1, ПК-7.2, ПК-7.3
33.	Инфракрасные средства обнаружения, назначение, состав, технические характеристики, принцип работы.	ПК-7.1, ПК-7.2, ПК-7.3
34.	Емкостные средства обнаружения, назначение, состав, технические характеристики, принцип работы.	ПК-7.1, ПК-7.2, ПК-7.3
35.	Вибрационные средства обнаружения, назначение, состав, технические характеристики, принцип работы.	ПК-7.1, ПК-7.2, ПК-7.3
36.	Комбинированные средства обнаружения, назначение, состав, технические характеристики, принцип работы.	ПК-7.1, ПК-7.2, ПК-7.3
37.	Быстро развертываемые средства обнаружения, назначение, состав, технические характеристики, принцип работы.	ПК-7.1, ПК-7.2, ПК-7.3
38.	Противоподкопные средства обнаружения, назначение, состав, технические характеристики, принцип работы.	ПК-7.1, ПК-7.2, ПК-7.3
39.	Охранно-пожарные технические средства предупреждения и нейтрализации воздействия.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
40.	Назначение и классификация средств сбора и обработки информации.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
41.	Устройство приемно-контрольных приборов и их основные характеристики.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
42.	Классификация телевизионных систем наблюдения.	ПК-3.1, ПК-3.2, ПК-3.3,

	Назначение и состав и технические характеристики телевизионных систем наблюдения.	ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
43.	Классификация мониторов систем наблюдения. Назначение и состав и технические характеристики мониторов систем видеонаблюдения.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
44.	Телевизионные камеры и мониторы. Устройства управления и коммутации видеосигналов.	ПК-7.1, ПК-7.2, ПК-7.3
45.	Типовые варианты телевизионных систем видеонаблюдения.	ПК-7.1, ПК-7.2, ПК-7.3
46.	Лицензирование и сертификация технических средств охраны и видеонаблюдения в области защиты информации.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
47.	Основные этапы проектирования системы обеспечения безопасности объекта техническими средствами охраны и видеонаблюдения.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
48.	Определение вероятности перехвата нарушителей спроектированной системой охраны (ошибки 1 и 2 рода).	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
49.	Моделирование объекта защиты от физического доступа посторонних лиц.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
50.	Моделирование угроз безопасности информации, возможных методов и способов реализации угроз.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,
51.	Контроль эффективности функционирования ИСО. Организационные, организационно-технические, технические методы контроля.	ПК-3.1, ПК-3.2, ПК-3.3, ПК-7.1, ПК-7.2, ПК-7.3, ПК-10.1, ПК-10.2, ПК-10.3,

Примерные тестовые задания – проверка сформированности компетенций – ПК-3, ПК-7, ПК-10

1. Инженерные средства охраны:

1) строительные конструкции здания (стены, потолки, двери, окна, металлические решётки и т.п.), внешние ограждающие конструкции (заборы, водоёмы, колючая проволока и т.п., сейфы, хранилище и т.п.): система контроля и управления доступом;

2) строительные конструкции здания (стены, потолки, двери, окна, металлические решётки и т.п.), внешние ограждающие конструкции (заборы, водоёмы колючая проволока и т.п.), сейфы. хранилища и т.п.: система телевизионного наблюдения;

3) строительные конструкции здания (стены, потолки, двери, окна, металлические решётки и т.п.), внешние ограждающие конструкции (заборы, водоёмы, колючая проволока и т.п.); сейфы, металлические шкафы и т.п.;

4) строительные конструкции здания (стены, потолки, двери, окна, металлические решётки и т.п.), внешние ограждающие конструкции (заборы, водоёмы, колючая проволока и т.п.).

2. Средства обнаружения, (извещатели) по принципу обнаружения делятся на:

1) отдельные предметы, закрытые помещения, открытые пространства, блокирование периметра, пожарные; точечные, линейные, поверхностные, объёмные; контактные;

2) акустические, оптико-электронные, микроволновые, вибрационные, ёмкостные, тепловые; отдельные предметы; закрытые помещения, открытые пространства, блокирование периметра, пожарные;

3) контактные, акустические, оптико-электронные, микроволновые, вибрационные, ёмкостные, тепловые, ионизационные, комбинированные;

4) точечные, линейные, поверхностные, объёмные.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источник

Основные

1. Доктрина информационной безопасности РФ. Утверждена Президентом Российской Федерации от 05.12.2016г. №646. [Электронный ресурс]: Режим доступа: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html, свободный. - Загл. с экрана.
2. Федеральный закон РФ Об информации, информационных технологиях и о защите информации» от 27 июля 2006 № 149-ФЗ. [Электронный ресурс]: Режим доступа: Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
3. Методические рекомендации Р 078-2019. «Инженерно-техническая укреплённость и оснащение техническими средствами охраны объектов и мест проживания и хранения имущества граждан, принимаемых под централизованную охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации». – М.: ФКУ «НИЦ «Охрана» Росгвардии, 2019. – 58 с. [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
4. Рекомендации Р 78.36.002-2010 «Выбор и применение систем охранных телевизионных». – М.: ФГУ НИЦ «Охрана» МВД России, 2010, – 183 с. [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
5. Методические рекомендации Р 063-2017 «Обследование объектов, охраняемых или принимаемых под охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации». – М.: ФГУ НИЦ «Охрана» Росгвардии, 2017, – 50 с [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
6. ТП 78.36.001-2014 Типовой рабочий проект «Система охранно-тревожной сигнализации. Комната хранения оружия». [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
7. ТП 78.36.002-2014 Типовой рабочий проект «Система охранно-тревожной сигнализации административное здание». [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
8. ТП 78.36.003-2014 Типовой рабочий проект «Система охранно-тревожной сигнализации. Трёхкомнатная квартира». [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
9. ТП 78.36.004-2014 Типовой рабочий проект «Система охранного телевидения». [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
10. ТП 78.36.005-2014 Типовой рабочий проект «Система контроля и управления доступом. Административное здание». [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.

Дополнительные

11. Список технических средств безопасности, удовлетворяющих «Единым требованиям к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации» (рекомендован решениями заседаний Технических советов ГУВО Росгвардии (Протокол № 2 от 15-16 мая 2019 г., протокол №3 от 22 июля 2019 г.)). – М.: ГУВО Росгвардии, 2019, – 79 с [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.

12. Единые требования к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии РФ. – М.: ГУВО Росгвардии, 2018, – 89 с [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
13. ГОСТ 26342-84: Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и размеры. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
14. ГОСТ 27990-88: Средства охранной, пожарной и охранно-пожарной сигнализации. Общие технические требования. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
15. ГОСТ 4.188-85: Система показателей качества продукции. Средства охранной, пожарной и охранно-пожарной сигнализации. Номенклатура показателей. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
16. ГОСТ Р 50775-95 (МЭК 60839-1-1-1988): Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
17. ГОСТ Р 50776-95 (МЭК 60839-1-4-1989): Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по эксплуатированию, монтажу и техническому обслуживанию. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
18. ГОСТ Р 50777-95/МЭК 60839-2-6-1990: Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 6. Пассивные оптико-электронные инфракрасные извещатели для закрытых помещений и открытых площадок. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
19. ГОСТ Р 50659-94/МЭК 60839-2-5-1990: Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 5. Радиоволновые доплеровские извещатели. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
20. ГОСТ Р 50658-94 (МЭК 60839-2-4-1990): Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 4. Ультразвуковые доплеровские извещатели для закрытых помещений. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
21. ГОСТ Р 52434-2005 (МЭК 60839-2-3-1987): Извещатели охранные оптико-электронные активные. Общие технические требования и методы испытаний. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
22. ГОСТ Р 51186-1998 Извещатели охранные звуковые пассивные для блокировки остеклённых конструкций в закрытых помещениях. Общие технические требования и методы испытаний. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
23. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
24. ГОСТ Р 51242-98 Конструкции защитные механические и электромеханические для дверных и оконных проёмов. Технические требования и методы испытаний на устойчивость к разрушающим воздействиям. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
25. ГОСТ Р 51558-2008 Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
26. ГОСТ Р 52435-2005 Технические средства охранной сигнализации. Классификация.

Общие технические требования и методы испытаний. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
27. ГОСТ Р 52436-2005 Приборы приёмно-контрольные охранной и охранно-пожарной сигнализации. Классификация. Общие технические требования и методы испытаний. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
28. ГОСТ Р 52551-2006 Системы охраны и безопасности. Термины и определения. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
29. ГОСТ Р 52651-2006 Извещатели охранные комбинированные радиоволновые с пассивными инфракрасными для закрытых помещений. Общие технические требования и методы испытаний. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
30. ГОСТ Р 52650-2006 Извещатели охранные линейные радиоволновые для периметров. Общие технические требования и методы испытаний. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
31. ГОСТ Р 52933-2008 Извещатели охранные поверхностные емкостные. Общие технические требования и методы испытаний. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
32. ГОСТ Р 53702-2009 Извещатели охранные вибрационные пассивные для блокировки строительных конструкций закрытых помещений и сейфов. Общие технические требования и методы испытаний. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
33. ГОСТ Р 53560-2009 Системы тревожной сигнализации. Источники электропитания. Классификация. Общие технические требования. Методы испытаний. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
34. ГОСТ Р 54126 - 2010 Оповещатели охранные. Классификация. Общие технические требования и методы испытаний. [Электронный ресурс] : Режим доступа : http://docs.cntd.ru/search/gostmain. – Загл. с экрана.
35. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. [Электронный ресурс]: Режим доступа: https://standartgost.ru/g/ГОСТ_Р_50922-2006, свободный. - Загл. с экрана.
36. ГОСТ Р 51275-2006 Защита информации. Объект информации. Общие положения. [Электронный ресурс]: Режим доступа: https://standartgost.ru/g/ГОСТ_Р_51275-2006, свободный. Загл. с экрана.
37. ГОСТ Р ИСО/МЭК 17799-2005 Практические правила управления информационной безопасностью. [Электронный ресурс]: Режим доступа: https://meganorm.ru/Index2/1/4293850/4293850664.htm6 свободный. Загл. с экрана.
38. ГОСТ Р ИСО/МЭК 15408-1 (15408-2, 15408-3) Критерии оценки безопасности информационных технологий. [Электронный ресурс]: Режим доступа: https://standartgost.ru/g/ГОСТ_Р_ИСО/МЭК 15408-1, свободный. Загл. с экрана.

Литература

Основная

1. *Торокин А.А*. Инженерно-техническая защита информации : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности / А. А. Торокин. – М. : Гелиос АРВ, 2005. – 958 с. : рис.,табл. - Библиогр.: с. 934-949. – ISBN 5-85438-140-0.
2. *Системы охранной* сигнализации: основы теории и принципы построения : учеб. пособие для студентов вузов, обучающихся по специальности 200700 – "Радиотехника" направления подгот. дипломир. специалистов 654200 - "Радиотехника" / Р. Г. Магауенов. - 2-е изд., перераб. и доп. - М. : Горячая линия-Телеком, 2008. - 493 с. : рис., табл. ; 22 см. - (Учебное пособие для вузов). - Библиогр.: с. 474-486 (237 назв.). - ISBN 978-5-9912-0025-7 : 297.00..

Дополнительная

3. Основные задачи и способы обеспечения безопасности автоматизированных систем обработки информации / Р. Г. Магауенов. - М. : Мир безопасности, 1997. - 108 с. : табл. - ISBN 5-89258-004-0 : 10.00.

Рекомендуемая литература (основная)

4. Словарь терминов и определений по информационной безопасности и защите информации [Электронный ресурс] : учебно-справочное пособие : для бакалавриата по направлению 090900.62 "Информационная безопасность" / Минобрнауки России, Федер. гос. бюджетное образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информ. наук и технологий безопасности, Фак. информац. систем и безопасности, Каф. информац. безопасности ; [сост.: Ищейнов В. Я., Мецатунян М. В.]. - Москва : РГГУ, 2014. - 117 с. - Режим доступа: http://elib.lib.rsuh.ru/elib/000009502. - Загл. с экрана.
5. Теория информации [Электронный ресурс] : учебно-методический комплекс для бакалавриата по направлению подготовки 090900 – «Информационная безопасность», профили: Организация и технология защиты информации ; Комплексная защита объектов информатизации / Минобрнауки России, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информ. наук и технологий безопасности, Фак. защиты информ., Каф. орг.-правовой защиты информ. ; [сост.: Е. И. Познякова, отв. ред.: А. А. Тарасов]. - Электрон. дан. - М. : РГГУ, 2013. - 27 с. - Режим доступа : http://elib.lib.rsuh.ru/elib/000007392. - Загл. с экрана.
6. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс] : Часть II. Организационное обеспечение информационной безопасности ; Учебно-методический комплекс для бакалавриата по направлению подготовки 090900 – «Информационная безопасность»; профили: Организация и технология защиты информации. Комплексная защита объектов информатизации. Ч. 2 / Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информ. наук и технологий безопасности, Фак. защиты информ., Каф. орг.-правовой защиты информ. ; [сост.: Г. А. Шевцова]. - Электрон. дан. - М. : РГГУ, 2012. - 55 с. - Режим доступа : http://elib.lib.rsuh.ru/elib/000007393.pdf. - Загл. с экрана.

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Информационный бюллетень Jet Info [Электронный ресурс]. – Электрон. дан. – [М., 2014]. – Режим доступа свобод.: http://www.jetinfo.ru/ .
2. Сайт НИЦ «Охрана» Росгвардии. – Режим доступа свобод.: http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html
3. Glossary Commander. Служба тематических толковых словарей [Электронный ресурс]. – Электрон. дан. - [М., 2008]. - Режим доступа свобод.: http://glossary.ru/ .
4. Сайт справочно-правовой системы по федеральному и региональным законодательствам России - Режим доступа свобод.: http://pravo.ru/
5. Информационный портал в области защиты информации Режим доступа свобод.: http://www.securitylab.ru
6. Портал ФСТЭК http://www.fstec.ru

7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимо:
1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должно быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

– обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

– для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

– письменные задания оформляются увеличенным шрифтом;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

– лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

– письменные задания выполняются на компьютере в письменной форме;

– экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

– в печатной форме увеличенным шрифтом;

– в форме электронного документа;

– в форме аудиофайла.

- для глухих и слабослышащих:

– в печатной форме;

– в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

– в печатной форме;
– в форме электронного документа;
– в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
  – устройством для сканирования и чтения с камерой SARA CE;
  – дисплеем Брайля PAC Mate 20;
  – принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
  – автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
  – акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
  – передвижными, регулируемыми эргономическими партами СИ-1;
  – компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий – проверка сформированности компетенций – ПК-3, ПК-7, ПК-10

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля за подготовкой студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для практических занятий, выдаваемые преподавателем на каждом занятии.

Целью практических занятий является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.

Тематика практических занятий соответствует программе дисциплины.

Практическая работа № 1 (6 часа). Обследование объекта – ПК-3, ПК-7, ПК-10

Цели работы:

– ознакомление с организацией обследования объектов на предмет инженерно-технической укреплённости элементов строительных конструкций;

– закрепление навыков выявления «уязвимых» с точки зрения несанкционированного проникновения мест и элементов строительных конструкций объектов;

– ознакомление с типовыми требованиями нормативных документов по организации инженерно-технической укреплённости элементов строительных конструкций охраняемых объектов;

– практическое освоение методов выработки предложений собственникам объектов по инженерно-технической укреплённости строительных конструкций охраняемых объектов.

Задания:

1. Изучить выданные в электронном виде:
- требования рекомендаций ГУВО Росгвардии Р-078-2019 и Р-063-2017;
- форму и пример составления акта обследования состояния технической укреплённости объекта (Р-063-2017).
2. Изучить выданные варианты планировок объектов с техническими описаниями их элементов технической укреплённости (в электронном виде, всего 17 вариантов).

Данные планировок с описаниями будут использованы и в последующих практических работах.

3. На основании Р-078-2019, и Р-063-2017 примера акта обследования, руководствуясь вышеуказанными требованиями по оформлению и содержанию актов, примером акта, определить категорию объекта и составить акт обследования состояния инженерно-технического укрепления объекта.
4. Составить отчёт о работе, в котором должны быть приведены план-схема объекта и акт об осмотре объекта с рекомендациями об ИТУ объекта

Указания по выполнению заданий:

1. Преподаватель раздаёт в электронном виде рекомендации ГУВО Росгвардии Р-078-2019 и Р-063-2017, описания помещений и поэтажные схемы помещений (как вариант – студенты сами рисуют планы в MS Visio).
2. Ответить на вопросы при защите работы

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, программным пакетом MS Office v.2010 и выше.

Список литературы:

1. Рекомендации Р 78.36.002-2010 «Выбор и применение систем охранных телевизионных». – М.: ФГУ НИЦ «Охрана» МВД России, 2010, – 183 с. [Электронный

ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.

2. Методические рекомендации Р 063-2017 «Обследование объектов, охраняемых или принимаемых под охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации». – М.: ФГУ НИЦ «Охрана» Росгвардии, 2017, – 50 с [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
3. Материалы лекций
4. А.А. Торокин Инженерно-техническая защита информации. Учебное пособие «Гелиос АРВ» 2005 - 960 с. полоч.индекс 600 Т61.

Практическая работа № 2 (8 часов). Разработка предложений по оснащению объекта охранной и тревожной сигнализацией и системой контроля и управления доступом – проверка сформированности компетенций – ПК-3, ПК-7, ПК-10

Цели работы:

– ознакомление с организацией построения систем охранно-тревожной сигнализации (ОТС), освоение навыков проектирования ОТС;

– закрепление навыков использования оборудования ОТС (извещателей, приёмно-контрольных приборов, оповещателей) для охраны объектов;

– ознакомление с типовыми требованиями нормативных документов по организации размещения, правил монтажа и установки из-вещателей и аппаратуры ОТС;

– ознакомление с аппаратурой ИСБ «Орион» НВП «Болид» и/или компании «Риэлта».

Задания:

1. Изучить выданные в электронном виде ГУВО Росгвардии Р-078-2019 и Р-063-2017 и типовые проекты решений ГУВО МВД России.
2. Изучить выданные варианты проектов охранно-тревожной сигнализации (в электронном виде).
3. Изучить технические характеристики современных технических средств охраны производства НВП «Болид» (https://bolid.ru) и ЗАО «Риэлта», г. Санкт-Петербург (https://rielta.ru)
4. На основании РД Р-078-2019, изученного лекционного материала и примера составления проектной документации (выданного в электронном виде) составить по имеющимся вариантам планировок, составленных в Практической работе № 1) структурную схему, поэтажные планы сетей ОТС, пояснительную записку, расчёт ёмкости резервного питания, спецификацию оборудования.

4.1. При составлении использовать MS Visio, стандартные условные обозначения извещателей и на выбор радиальное распределение шлейфов или двухпроводную адресную линию.

4.2. При использовании технических средств охраны применять оборудование НВП «Болид» и ЗАО «Риэлта» г. Санкт-Петербург. (Возможно использование других технических средств по согласованию с преподавателем).

5. Составить отчёт о работе, в котором должны быть приведены копии документов, приведённые в п. 4

Указания по выполнению заданий:

1. Преподаватель раздаёт в электронном виде рекомендации ГУВО Росгвардии Р-078-2019 и Р-063-2017, описания помещений и поэтажные схемы помещений (как вариант – студенты сами рисуют планы в MS Visio или аналогичной программе).
2. Ответить на вопросы при защите работы

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, программным пакетом MS Office v.2010 и выше.

Список литературы:

1. Рекомендации Р 78.36.002-2010 «Выбор и применение систем охранных телевизионных». – М.: ФГУ НИЦ «Охрана» МВД России, 2010, – 183 с. [Электронный

ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
2. Методические рекомендации Р 063-2017 «Обследование объектов, охраняемых или принимаемых под охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации». – М.: ФГУ НИЦ «Охрана» Росгвардии, 2017, – 50 с [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
3. ТП 78.36.001-2014 Типовой рабочий проект «Система охранно-тревожной сигнализации. Комната хранения оружия». [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
4. ТП 78.36.002-2014 Типовой рабочий проект «Система охранно-тревожной сигнализации административное здание». [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
5. ТП 78.36.003-2014 Типовой рабочий проект «Система охранно-тревожной сигнализации. Трёхкомнатная квартира». [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
6. ТП 78.36.005-2014 Типовой рабочий проект «Система контроля и управления доступом. Административное здание». [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
7. Материалы лекций
8. А.А. Торокин Инженерно-техническая защита информации. Учебное пособие «Гелиос АРВ» 2005 - 960 с. полоч.индекс 600 Т61.

Практическая работа № 3 (8 часов). Разработка предложений по оснащению объекта системой охранного телевидения – проверка сформированности компетенций – ПК-3, ПК-7, ПК-10

Цели работы:

– ознакомление с организацией построения систем охранного телевидения, освоение навыков проектирования;

– ознакомление с типовыми требованиями нормативных документов по организации размещения, правил монтажа и установки аппаратуры телевизионного наблюдения;

– ознакомление с методикой проведения необходимых расчётов при оборудовании объектов системами телевизионного наблюдения.

Задания:

1. Выбрать видеокамеры с сайта https://bolid.ru/production/cctv/network_camera/ с учётом места установки (условий работы) и разместить видеокамеры на схеме объекта с учётом охраны внешнего периметра здания.
2. Рассчитать поля зрения камер и минимальную разрешаемую деталь для каждой камеры и сделать вывод о том, следует ли оставить эту камеру или изменить параметры объектива.
3. Выбрать регистраторы с раздела сайта https://bolid.ru/production/cctv/nvr/ и коммутаторы с раздела https://bolid.ru/production/cctv/switche/.
4. Необходимое количество регистраторов разместить на посту охраны. Коммутаторы на этажах на стойках.
5. Нарисовать схему системы охранного телевидения объекта (ТК, необходимое количество коммутаторов и регистраторов).
6. Рассчитать ёмкость каждого видеорегистратора с учётом его ТТХ.
7. Составить отчёт о работе, в котором должны быть приведены копии документов, приведённые в пп. 4…6

7.1 При составлении использовать MS Visio (или аналогичной программе), стандартные условные обозначения извещателей.

7.2. При использовании технических средств охраны применять оборудование НВП «Болид» и ЗАО «Риэлта» г. Санкт-Петербург. (Возможно использование других технических средств по согласованию с преподавателем).

Указания по выполнению заданий:

1. Преподаватель раздаёт в электронном виде:
– примеры проектной документации (листы проекта, поэтажные планы, структурная схема, пояснительная записка) и типовой проект ТП 78.36.004-2014 в электронном виде;
– варианты планировок объектов с техническими описаниями их элементов технической укреплённости, применяемые в работе № 1.
2. Ответить на вопросы при защите работы

Список литературы:

1. ТП 78.36.004-2014 Типовой рабочий проект «Система охранного телевидения». [Электронный ресурс] : Режим доступа : http://www.nicohrana.ru/normativno-tehnicheskaya-dokumentaciya.html. – Загл. с экрана.
2. Материалы лекций
3. А.А. Торокин Инженерно-техническая защита информации. Учебное пособие «Гелиос АРВ» 2005 – 960 с. полоч.индекс 600 Т61.

По результатам практических занятий обучающиеся составляют отчёты. Отчёт составляется в электронной форме с использованием ПКП MS Office и выше и передаётся преподавателю посредством оговорённой формы связи.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Интегрированные системы охраны» реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профиль подготовки – Безопасность автоматизированных систем) кафедрой комплексной защиты информации.

Цель дисциплины: профессиональная подготовка студентов, необходимая для освоения методов и технологий, связанных с обеспечением безопасности объекта охраны от физического доступа посторонних лиц.
Задачи:

- получение систематизированных знаний о современных концепциях, методах и технологиях обеспечения безопасности объекта охраны от физического доступа посторонних лиц;
- изучение теоретических основ обеспечения безопасности объекта охраны от физического доступа посторонних лиц;
- формирование умений использовать современные достижения в области обеспечения безопасности объекта охраны от физического доступа посторонних лиц при реализации своей профессиональной деятельности;
- владение практическими навыками, применения современных методами, сил и средств в обеспечении безопасности объекта охраны от физического доступа посторонних лиц;
- развитие аналитического мышления, умения строго излагать свои мысли, развитие способностей к обобщению и анализу информации, постановке целей и выбору путей ее достижения.

Дисциплина направлена на формирование следующих компетенций:

- ПК-3 – Способен управлять защитой информации в автоматизированных системах
  - ПК-3.1 – Знает основные методы управления защитой информации, информационные ресурсы автоматизированных систем, подлежащие защите; основные угрозы безопасности информации, модели нарушителя в автоматизированных системах
  - ПК-3.2 – Умеет разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем; классифицировать и оценивать угрозы безопасности информации; оценивать информационные риски в автоматизированных системах
  - ПК-3.3 – Владеет навыками составления комплекса правил, процедур, практических приёмов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе
- ПК-7 – Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
  - ПК-7.1 – Знает разработку концепции средств и систем информатизации в защищённом исполнении, разработку технического задания на средство и/или систему информатизации в защищённом исполнении
  - ПК-7.2 – Умеет разрабатывать конструкторскую и технологическую документацию на средство и/или систему информатизации в защищённом исполнении
  - ПК-7.3 – Владеет навыками разработки рабочей и эксплуатационной документации на средства и системы информатизации в защищённом исполнении
- ПК-10 – Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

- ПК-10.1 – Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
- ПК-10.2 – Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации
- ПК-10.3 – Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации

В результате освоения дисциплины обучающийся должен:
Знать: состав и порядок разработки нормативных документов по обеспечению безопасности объектов охраны; состав, структуру и принципы работы интегрированных систем охраны и их элементов; требования нормативных и руководящих документов РФ по обеспечению безопасности объектов охраны; модели нарушителя объекта охраны, на котором размещена АС.
Уметь: организовать работу по обеспечению безопасности объектов охраны от воздействия источников угроз и реализации угроз; выбирать технические средства охраны, системы контроля и управления доступом, системы видеонаблюдения для выполнения профессиональных задач; разрабатывать нормативные документы по обеспечению безопасности объектов охраны, на которых размещена АС, от физического доступа посторонних лиц.
Владеть: практическими навыками по использованию нормативных и руководящих документов в организации работ по защите объектов охраны; навыками проектирования интегрированных систем охраны; навыками безопасного использования технических средств в профессиональной деятельности; навыками по моделированию источников угроз и угроз безопасности объектов охраны, на которых размещена АС.

По дисциплине предусмотрена промежуточная аттестация в форме зачёта.

Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.

Приложение 2

УТВЕРЖДЕНО
Протокол заседания кафедры
№_____ от_____

ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе дисциплины__ Интегрированные системы охраны ___

по направлению подготовки __Информационная безопасность _____

на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:
(элемент рабочей программы)
1.1. ……..;
1.2. ……...;
…
1.9. …… .

2. В _____ вносятся следующие изменения:
(элемент рабочей программы)
2.1. ……..;
2.2. ……...;
…
2.9. …… .

3. В _____ вносятся следующие изменения:
(элемент рабочей программы)
3.1. ……..;
3.2. ……...;
…
3.9. …… .

Составитель _____ /_____ /
подпись расшифровка подписи
« ____ » _____ 201__