МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение инклюзивного высшего образования

**«Российский государственный
университет социальных технологий»**

(ФГБОУ ИВО «РГУ СоцТех»)

УТВЕРЖДАЮ

Проректор по образовательной деятельности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Образовательная программа направления подготовки
09.04.03 «Прикладная информатика»
шифр, наименование

Б1.В.01 «Дисциплины(модули)», часть, формируемая участниками образовательных отношений, Дисциплины(модули) по выбору

Направленность (профиль)
Прикладная информатика в информационной сфере

Квалификация (степень) выпускника: магистр

Форма обучения очная

Курс 1 семестр 2

Москва 2024

Содержание

1.1. Цель и задачи изучения учебной дисциплины (модуля)

Основными целями преподавания дисциплины являются:

• формирование у студентов знаний по основам инженерно-технической защиты информации, а также навыков и умения в применении знаний для конкретных условий;

• развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.

Основными задачами изучения дисциплины являются:

• получение теоретических знаний о концепции инженерно-технической защиты информации;

• дать знания по физическим, организационным основам инженерно-технической защиты информации;

• получение знаний о средствах и методах добывания и средствах и методах защиты конфиденциальной информации;

• методическое обеспечение инженерно-технической защиты информации.

Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ПК-1 Способен использовать и развивать методы научных исследований и инструментария в области проектирования и управления информационными системами в прикладных областях	ПК-1.1 Знает основные подходы, методы в области проектирования и управления информационными системами в прикладных областях; возможности современных инструментальных средств для проектирования и управления информационными системами в прикладных областях; способы представления научно-технической информации.
	ПК-1.2 Умеет использовать и развивать методы научных исследований в области проектирования и управления информационными системами в прикладных областях; анализировать иностранные источники в области проектирования и управления ИС в прикладных областях; использовать и развивать методы инструментарий в области проектирования и управления информационными системами в прикладных областях; правильно подготавливать научно-технические отчеты; оформлять результаты исследований в виде статей и докладов на научных конференциях в предметной области.
	ПК-1.3 Владеет практическими навыками использования и развития инструментальных средств в области проектирования и управления информационными системами в прикладных областях; навыками работы в системах поиска информации, текстовых процессорах, электронных таблицах, базах данных и системах подготовки презентаций.
ПК-5 Способен исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций	ПК-5.1 Знает различные научные подходы к автоматизации информационных процессов и информатизации предприятий и организаций; процесс подготовки информации к принятию управленческих решений; тенденции развития автоматизации управления промышленными предприятиями.
	ПК-5.2 Умеет провести алгоритмизацию конкретной управленческой задачи; применять различные научные подходы к автоматизации информационных процессов и информатизации предприятий и организаций.

	ПК-5.3 Владеет навыками применения типовых подходов, применяемых при анализе, планировании и оперативном управлении деятельностью промышленного предприятия; навыками исследования применения различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций на основе приобретенных знаний и умений и их применения в нетипичных ситуациях.

1.2. Место дисциплины (модуля) в структуре образовательной программы направления подготовки 09.04.03 «Прикладная информатика (уровень магистратуры)»

Для успешного освоения дисциплины студент должен иметь базовую подготовку по информатике и математике в пределах программы средней школы, а также дисциплины младших курсов, такие как

- Математический анализ
- Теория вероятностей и математическая статистика
- Информационные операции и атаки в распределенных информационных системах

Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее

- Разработка и эксплуатация защищенных автоматизированных систем
- Методы проектирования защищенных распределенных информационных систем
- Управление рисками в распределенных информационных системах

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы в соответствии с формами обучения

Объем дисциплины «Техническая защита информации» составляет 5 зачетных единиц/180 часов:

Вид учебной работы	Всего, часов	Очная форма Курс, часов 1 курс, 2 сем.
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	*42*	*42*
Лекции	12	12
Практические занятия	30	30
Лабораторные занятия		
Самостоятельная работа обучающихся	102	102
Промежуточная аттестация (подготовка и сдача), всего:		
Контрольная работа	36	36
Курсовая работа		
Зачет с оценкой		
Экзамен	2	2
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	180\5	180\5

2.2. Содержание дисциплины по темам (разделам)

№ п/п	Наименование раздела (темы)	Содержание раздела (тематика занятий)	Формируемые компетенции (индекс)
1.	Технические каналы утечки информации	Системный подход к защите информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы.	ПК-1,ПК-5
2.	Способы и средства защиты информации от утечки по техническим каналам	Основные концептуальные положения технической защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации.	ПК-1,ПК-5
3	Методы и средства контроля эффективности технической защиты информации	Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности инженерно-технической защиты информации. Виды зон контроля. Требования по защите информации от 2 7 утечки по техническим каналам. Виды технического контроля.	ПК-1,ПК-5
4	Организация технической защиты информации	Государственная система защиты информации. Основные задачи, структура и характеристика государственной системы противодействия технической защите. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации. Самостоятельное изучение. Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств	ПК-1,ПК-5

2.3. Разделы дисциплин и виды занятий

№ п/п	Наименование темы дисциплины	Лекционные занятия	Практические занятия	Самостоятельная работа	Контроль	Всего часов	Формы текущего контроля успеваемости
1.	Технические каналы утечки информации	3	7	25	9	35	Устный опрос
2.	Способы и средства защиты информации от утечки по техническим каналам	3	8	24	9	35	Устный опрос
3	Методы и средства контроля	3	7	29	9	33	Устный опрос

	эффективности технической защиты информации						
4	Организация технической защиты информации	3	8	24	9	35	Устный опрос
Экзамен			2				
	Итого:	12	30	102	36	180\5	

2.4. Планы теоретических (лекционных) занятий

Тема лекции. Вопросы, отрабатываемые на лекции	**Всего часов**
Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации.	2
Особенности информации как предмета защиты. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ.	2
Моделирование инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты	2
Методические рекомендации по оценке эффективности защиты информации. Способы оценки эффективности охраны объектов защиты. Оценка эффективности защиты видовых признаков объектов наблюдения. Способы оценки безопасности речевой информации в помещении. Способы определения уровней опасных сигналов на выходах основных и вспомогательных технических средств. Способы оценки размеров зон I и II.	2
Физические основы защиты информации от технических разведок. Классификация средств технических разведок по виду носителя. Типовые задачи технических разведок. Принципы действия аппаратуры технических разведок. Классификация методов и средств защиты информации от технических разведок.	2
Методы инженерной защиты и технической охраны объектов. Классификация методов инженерной защиты и технической охраны объектов защиты. Модели злоумышленника. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления. Комплекс технических средств охраны.	2

2.5. Планы практических (семинарских) занятий

Тема практического занятия. Вопросы, отрабатываемые на практическом занятии	Всего часов
Оценка пропускной способности канала утечки информации.	5
Оценка дальности передачи информации по каналу утечки	5
Разработка алгоритма функционирования для типовой подсистемы защиты информации для типовых ТКС.	5
Законы распределения случайных величин. Статистические оценки и их точность.	5
Разработка матрицы конфликтного взаимодействия для типовых ТКС.	5
Формулировка стратегий защиты для типовой ТКС. Разработка тактик и стратегии защиты, контроля для типовой ТКС с учетом целевого назначения ТКС.	5

2.6. Планы лабораторных работ – не предусмотрено.

2.7. Задания для самостоятельного изучения

Задания, вопросы, для самостоятельного изучения (задания)	Всего часов
Характеристика и возможности оптических, акустических радиоэлектронных и материально-вещественных каналов утечки информации.	15
Основные параметры системы защиты информации.	10
Основные показатели среды распространения сигналов, влияющие на дальность технических каналов утечки и качество информации на его выходе.	20
Показатели эффективности инженернотехнической защиты информации.	20
Оценка качества статистической модели.	17
Основные положения теории нестационарных моментов марковских сетей.	20

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ИНВАЛИДНОСТЬЮ И ОВЗ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться следующих варианты восприятия учебной информации с учетом их индивидуальных психофизических

особенностей, в том числе с применением электронного обучения и дистанционных технологий:

1) для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.
2) для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.
3) для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение дисциплины для организации самостоятельной работы студентов (содержит перечень основной литературы, программного обеспечения и Интернет-ресурсы).

В распоряжении преподавателей и обучающихся имеется основное необходимое материально-техническое оборудование, Интернет-ресурсы, доступ к полнотекстовым электронным базам, книжный фонд библиотеки Московского государственного гуманитарно-экономического университета.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Перечень основной литературы

1. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2023. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1912992
2. Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2023. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1899016
3. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2022. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1861659

5.2 Перечень дополнительной литературы

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537247

2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537000
3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544290
4. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2024. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536132
5. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2024. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536902

5.3 Программное обеспечение

Текстовый редактор
Microsoft Windows
Microsoft Office
7-Zip
AcrobatReader

5.4 Электронные ресурсы

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Федеральный портал «Российское образование www.edu.ru
6. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
7. Российский биометрический портал www.biometrics.ru
8. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
9. Сайт Научной электронной библиотеки www.elibrary.ru
10. Электронная библиотека «Знаниум»: https://znanium.com

11. Электронная библиотека «Юрайт»: https://urait.ru

12. Электронно-библиотечная система «Лань»: https://e.lanbook.com/

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий	Перечень оборудования и технических средств обучения
1.	Лекционная аудитория	Персональный компьютер, мультимедийный проектор
2.	Компьютерный класс	Персональные компьютеры (IBM PC-совместимые) под управлением ОС Microsoft Windows, компьютерная сеть, доступ в сеть Интернет

7. ОЦЕНКА КОМПЕТЕНЦИЙ ПО ИЗУЧАЕМОЙ ДИСЦИПЛИНЕ

№	**Критерии оценки**			
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	ЗНАТЬ			
1	Студент не усвоил следующие знания: технические каналы утечки информации, возможности технических средств перехвата информации, способы и средства защиты информации от утечки по техническим каналам, организацию защиты информации от утечки по техническим каналам на объектах информатизации, основы физической защиты объектов информатизации	Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания по темам: технические каналы утечки информации, возможности технических средств перехвата информации, способы и средства защиты информации от утечки по техническим каналам,	Студент способен самостоятельно выделять главные положения в изученном материале. Знает: технические каналы утечки информации, возможности технических средств перехвата информации, способы и средства защиты информации от утечки по техническим каналам, организацию защиты информации от утечки по техническим	технические каналы утечки информации, возможности технических средств перехвата информации, способы и средства защиты информации от утечки по техническим каналам, организацию защиты информации от утечки по техническим каналам на объектах информатизации, основы физической защиты объектов

			каналам на объектах информатизации	информатизации
УМЕТЬ				
2	Студент не умеет пользоваться нормативными документами по противодействию технической разведке, анализировать и оценивать угрозы информационной безопасности объекта	Студент испытывает затруднения при оценивании применимости того или иного отечественного стандарта. оценивать угрозы информационной безопасности объекта, Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	Студент умеет использовать стандартные программно-аппаратные средства, реализующие тот или иной стандарт криптографическог о протокола; Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	Студент умеет самостоятельно Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации. Пользоваться профессиональной документацией на государственном и иностранном яз. пользоваться нормативными документами по противодействию технической разведке, анализировать и оценивать угрозы информационной безопасности объекта
ВЛАДЕТЬ				
3	Студент не владеет следующими знаниями: основные угрозы информации , основные методы и средства защиты информации, основные виды организационных методов защиты	Студент владеет методикой установки, монтажа и настройки технических средств защиты информации; техническом обслуживании технических средств	Студент владеет методикой установки, монтажа и настройки технических средств защиты информации; техническим обслуживанем	Студент владеет методикой установки, монтажа и настройки технических средств защиты информации; техническим

	информации	защиты информации;	технических средств защиты информации; применением основных типов технических средств защиты информации;	обслуживанем технических средств защиты информации; применением основных типов технических средств защиты информации; выявлением технических каналов утечки информации
	Компетенции или их части не сформированы.	Компетенции или их части сформированы на базовом уровне.	Компетенции или их части сформированы на среднем уровне.	Компетенции или их части сформированы на высоком уровне.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Интерактивные образовательные технологии, используемые в аудиторных занятиях и самостоятельной работе обучающихся

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
1	Л	Лекция-беседа, ТСО (мультимедийный проектор, презентации PowerPoint)	12
	ПР	Практикум на ЭВМ, проблемный метод, взаимообучение	30
	ЛР	Не предусмотрены	
	КР	Устный опрос	36
	Сам.работа	ЭБС, дистанционные консультации, взаимообучение в студенческой среде	102
Итого:			180

9. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

9.1. Организация входного, текущего и промежуточного контроля обучения

Входное тестирование – не предусмотрено.

Текущий контроль – устный опрос, защита отчетов по практическим работам, работа на компьютерах в парах, презентация в режиме диалога, работа в парах.

Промежуточная аттестация – экзамен

9.2. Тематика рефератов, проектов, творческих заданий, эссе и т.п.

Не предусмотрены.

9.3. Курсовая работа

Не предусмотрено.

9.4. Вопросы к экзамену

1. Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации.
2. Представление сил и средств защиты информации в виде системы.
3. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации.
4. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности
распространения акустических сигналов в помещениях.
5. Распространение оптических сигналов в атмосфере и в светопроводах.
6. Распространение радиосигналов различных диапазонов в пространстве и по направляющим
линиям связи.
7. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации.
8. Принципы защиты информации техническими средствами.
9. Основные направления инженерно-технической защиты информации.
10. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации.
11. Демаскирующие признаки объектов наблюдения, сигналов и веществ.
12. Основные теоремы теории вероятностей.
13. Моделирование случайных величин и их законы распределения.
14. Статистические оценки и их точность.
15. Аппроксимация результатов статистического моделирования.
16. Основные этапы проектирования и оптимизации системы инженерно-технической защиты
информации.
17. Принципы моделирования объектов защиты.
18. Моделирование угроз безопасности информации. Методические рекомендации по выбору
рациональных вариантов защиты.
19. Задачи защиты информации ТКС в условиях конфликта.
20. Понятие конфликта. Способы разрешения конфликта в ТКС.
21. Стратегии противоборствующих сторон в динамике развития информационного конфликта
ТКС с системами воздействия.

22. Понятия стратегия, тактика обеспечения защиты информации, воздействия на ТКС.
23. Конфликтная матрица реализации стратегий (тактик) защиты и воздействия.
24. Виды контроля эффективности инженерно-технической защиты информации. Виды зон контроля.
25. Требования по защите информации от утечки по техническим каналам. Виды технического контроля.
26. Способы оценки эффективности охраны объектов защиты. Оценка эффективности защиты
видовых признаков объектов наблюдения.
27. Способы оценки безопасности речевой информации в помещении.
28. Способы определения уровней опасных сигналов на выходах основных и вспомогательных технических средств.
29. Способы оценки размеров зон I и II.
30. Основные задачи, структура и характеристика государственной системы противодействия технической защите.
31. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации.
32. Классификация средств технических разведок по виду носителя. Типовые задачи технических разведок.
33. Принципы действия аппаратуры технических разведок.
34. Классификация методов и средств защиты информации от технических разведок.
35. Классификация методов инженерно-технической защиты информации.
36. Инженерная защита и техническая охрана объектов.
37. Пространственное, энергетическое и структурное скрытие информации и ее носителей.
38. Дезинформирование, как метод скрытия.
39. Математическая модель канала утечки информации применительно к техническим разведкам.
40. Пространственное скрытие объектов наблюдения и сигналов.
41. Структурное и энергетическое скрытие объектов наблюдения.
42. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение.
43. Энергетическое скрытие радио и электрических сигналов.
44. Классификация методов инженерной защиты и технической охраны объектов защиты.
45. Инженерные конструкции. Автономные и централизованные системы охраны
46. Модели злоумышленника.
47. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления.
48. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара.
49. Комплекс технических средств охраны

9.6. Контроль освоения компетенций

Вид контроля	**Контролируемые темы (разделы)**	**Компетенции, компоненты которых контролируются**
Устный опрос	*1-4*	ПК-1,ПК-5

1.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Номер и дата протокола заседания кафедры	Перечень измененных пунктов	Подпись заведующего кафедрой