

УТВЕРЖДАЮ

Первый проректор, проректор по
УР

_____ А.Е. Рудин

«31» __ 10 __ 2023 года

Рабочая программа дисциплины

Б1.О.12

Современные технические средства охраны объектов

Учебный план: 2024-2025 10.04.01 ИИТА ПСЗИНП ОО №2-1-159.plx

Кафедра: **20** Интеллектуальных систем и защиты информации

Направление подготовки:
(специальность) 10.04.01 Информационная безопасность

Профиль подготовки: Проектирование систем защиты информации на предприятии
(специализация)

Уровень образования: магистратура

Форма обучения: очная

План учебного процесса

Семестр (курс для ЗАО)		Контактная работа обучающихся		Сам. работа	Контроль, час.	Трудоём- кость, ЗЕТ	Форма промежуточной аттестации
		Лекции	Практ. занятия				
1	УП	34	34	41,5	34,5	4	Экзамен
	РПД	34	34	41,5	34,5	4	
Итого	УП	34	34	41,5	34,5	4	
	РПД	34	34	41,5	34,5	4	

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.04.01 Информационная безопасность, утвержденным приказом Минобрнауки России от 26.11.2020 г. № 1455

Составитель (и):

кандидат технических наук, Доцент

Бусыгин К.Н.

Старший преподаватель

Морозов С.К.

От кафедры составителя:

Заведующий кафедрой интеллектуальных систем и
защиты информации

Макаров Авинир

Геннадьевич

От выпускающей кафедры:

Заведующий кафедрой

Макаров Авинир

Геннадьевич

Методический отдел:

1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1 Цель дисциплины: Формирование у обучающихся компетенций в области охраны объектов современными техническими средствами, проектирования инженерно-технических систем защиты на предприятии

1.2 Задачи дисциплины:

- показать типы и классы технических средств охраны объектов;
- научить пользоваться методикой анализа и выбора оптимальных технических решений в области проектирования систем защиты информации;
- рассмотреть демаскирующие признаки объектов наблюдения и сигналов; опасные сигналы и их источники;
- рассмотреть структуру, классификацию и основные характеристики технических каналов утечки информации;
- продемонстрировать возможности видов технической разведки, концепцию и методы инженерно-технической защиты информации.

1.3 Требования к предварительной подготовке обучающегося:

Предварительная подготовка предполагает создание основы для формирования компетенций, указанных в п. 2, при изучении дисциплин:

Дисциплина базируется на компетенциях, приобретенных на предыдущем уровне образования

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-2: Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности
Знать: ассортимент, области применения и особенности настройки и эксплуатации доступных в РФ технических средств охраны объектов
Уметь: выбирать технические средства охраны объекта, при проектировании систем безопасности в соответствии с законодательными и техническими требованиями и в зависимости от специфики объекта охраны
Владеть: навыками составления, визуализации и презентации технического задания на применение технических средств охраны при проектировании систем безопасности предприятия

3 РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Наименование и содержание разделов, тем и учебных занятий	Семестр (курс для ЗАО)	Контактная работа		СР (часы)	Инновац. формы занятий	Форма текущего контроля
		Лек. (часы)	Пр. (часы)			
Раздел 1. Основные положения инженерно - технической защиты информации	1					0
Тема 1. Предмет и задачи технической защиты информации. Основные параметры системы защиты информации Практическое занятие: Системный подход при решении задач инженерно - технической защиты информации		2	2	4		
Тема 2. Общие положения защиты информации техническими средствами. Задачи и требования к способам и средствам защиты информации техническими средствами. Практическое занятие: Принципы системного анализа проблем инженерно- технической защиты информации. Классификация способов и средств защиты информации		4	4	4		

<p>Тема 3. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке</p> <p>Практическое занятие: Содержательный анализ нормативные и методические документы по защите информации и противодействию технической разведке</p>	2	2	4	ИЛ	
<p>Тема 4. Информация как предмет защиты. Свойства, виды, источники и носители защищаемой информации</p> <p>Практическое занятие: Демаскирующие признаки объектов наблюдения сигналов и веществ. Понятие об опасном сигнале, источники опасных сигналов основные и вспомогательные технические средства и системы</p>	2	4	4		
<p>Раздел 2. Технические каналы утечки информации и организация их защиты</p>					О
<p>Тема 5. Понятие и особенности утечки информации. Структура, характеристика и классификация каналов утечки информации. Средства инженерной защиты и технической охраны. Средства предотвращения утечки информации по техническим каналам</p> <p>Практическое занятие: Технические каналы утечки видовой информации.</p> <p>Практическое занятие: Каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации.</p>	2	4	2	ИЛ	
<p>Тема 6. Каналы утечки речевой информации. Акустические каналы. Виброакустические каналы. Акустоэлектрические каналы. Оптико-электронные каналы. Параметрические каналы.</p> <p>Практическое занятие: Организация защиты речевой информации. Пассивные средства защиты выделенных помещений. Аппаратура и способы активной защиты помещений от утечки речевой информации.</p>	2	2	2		
<p>Тема 7. Несанкционированный доступ к информации, обрабатываемой средствами вычислительной техники. Каналы утечки информации при ее передаче по каналам связи. Технические каналы утечки информации, возникающей при работе вычислительной техники за счет ПЭМИН.</p> <p>Практическое занятие: Организация защиты информации от утечки возникающей при работе вычислительной техники за счет ПЭМИН. Методология защиты информации от утечки за счет ПЭМИН.</p>	2	2	2		

Раздел 3. Средства обнаружения каналов утечки информации					
Тема 8. Классификация технической разведки. Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Практическое занятие: Характеристики индикаторов электромагнитных излучений. Радиочастотомеров, сканирующих приемников, селективных вольтметров, анализаторов спектра	4	2	2		О
Тема 9. Устройства для перехвата информации и признаки их установки. Нелинейные локаторы. Характеристики и функции нелинейных локаторов и селективных металлодетекторов. Досмотровая техника состав и область применения. Практическое занятие: Методы скрытия информации и ее носителей. Пространственное скрытие объектов наблюдения и сигналов. Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции из звукопоглощения.	4	2	4	ИЛ	
Тема 10. Организованные каналы утечки (съема) информации –закладные устройства. Закладные устройства с проводными каналами передачи. Типы закладных устройств. Практическое занятие: Методы обнаружения закладных устройств и паразитных излучений с применением широкополосных индикаторов и сканирующих приемников. Мониторинг эфира. Проблемы, возникающие при обнаружении закладных устройств	4	2	4		
Раздел 4. Основы физической защиты объектов информатизации					
Тема 11. Проектирование системы физической защиты объекта охраны. Основные положения и методы. Практическое занятие: Виды угроз и примеры технических средств физической безопасности	2	2	4		
Тема 12. Организация физической защиты объектов информатизации. Телевизионная система оценки сигнала тревоги. Практическое занятие: Установка и настройка устройств видеонаблюдения. Настройка сигнализации в помещении. Классификация датчиков охранной сигнализации. Простейшая модель охранной сигнализации	2	4	3,5	ИЛ	О

Тема 13. Государственная система защиты информации. Специальные проверки. Порядок проведения специальной проверки технических средств		2	2	2		
Практическое занятие: Контроль эффективности инженерно-технической защиты информации. Методы технического контроля.						
Итого в семестре (на курсе для ЗАО)		34	34	41,5		
Консультации и промежуточная аттестация (Экзамен)		10		24,5		
Всего контактная работа и СР по дисциплине		78		66		

4 КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Курсовое проектирование учебным планом не предусмотрено

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1 Описание показателей, критериев и системы оценивания результатов обучения

5.1.1 Показатели оценивания

Код компетенции	Показатели оценивания результатов обучения	Наименование оценочного средства
ОПК-2	Перечисляет современные технические средства охраны объекта, классифицируя их по области применения и/или принципу действия. При проектировании систем инженерно-технологической защиты информации руководствуется законодательными, нормативными и техническими документами. Формирует отчетные документы по проектированию и визуализации разработанной системы	вопросы для устного собеседования и практико-ориентированные задания

5.1.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
5 (отлично)	Полный, исчерпывающий ответ, явно демонстрирующий глубокое понимание предмета и широкую эрудицию в оцениваемой области. Критический, оригинальный подход к материалу.	не предусмотрена
4 (хорошо)	Ответ стандартный, в целом качественный, основан на всех обязательных источниках информации. Присутствуют небольшие пробелы в знаниях или несущественные ошибки.	не предусмотрена
3 (удовлетворительно)	Ответ неполный, основанный только на лекционных материалах. При понимании сущности предмета в целом – существенные ошибки или пробелы в знаниях сразу по нескольким темам, незнание (путаница) важных терминов.	не предусмотрена
2 (неудовлетворительно)	Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные грубые ошибки. Попытка списывания, использования неразрешенных технических устройств или пользования подсказкой другого человека (вне зависимости от успешности такой попытки).	не предусмотрена

5.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

5.2.1 Перечень контрольных вопросов

№ п/п	Формулировки вопросов
Семестр 1	
1	Определение технического средства охраны.
2	Виды устройств идентификации и аутентификации в СКУД.
3	Характеристики технических каналов утечки информации. Общая классификация технических каналов утечки. Основные определения.
4	Методы скрытия информации и ее носителей
5	Особенности купольной камеры наблюдения. В каких случаях обусловлена установка такого типа камер? Типы микроволновых извещателей.
6	Что такое средство нейтрализации угроз?
7	Определение охранного извещателя (датчика)
8	Характеристика технической защиты информации как области информационной безопасности
9	Основные проблемы технической защиты информации
10	Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки
11	Основные этапы и процессы добывания информации технической разведкой
12	Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации
13	Средства технической разведки
14	Организованные каналы утечки (съема) информации
15	Методы обнаружения каналов утечки по ПЭМИН и через закладные устройства
16	Методы инженерной защиты и технической охраны объектов
17	Классификация способов инженерной защиты и технической охраны объектов
18	Основные параметры системы защиты информации
19	Принципы защиты информации техническими средствами
20	Основные направления технической защиты информации
21	Показатели эффективности технической защиты информации
22	Источники опасных сигналов. Понятие об опасном сигнале
23	Основные и вспомогательные технические средства и системы как источники опасных сигналов
24	Что такое подсистема физической безопасности объекта в составе комплексной системы защиты информации?
25	Какие технические средства защиты могут предотвратить реализацию лазерного канала утечки речевой информации?
26	Как Вы понимаете принцип эшелонирования зон безопасности?
27	Средства предотвращения утечки информации по техническим каналам
28	Технические каналы утечки информации, обрабатываемой основными техническими средствами и системами.
29	Электромагнитные каналы утечки информации. Перехват побочных электромагнитных излучений ТСПИ средствами разведки ПЭМИН
30	Электрические каналы утечки информации. Перехват наведенных информативных сигналов.
31	Параметрические каналы утечки информации. Перехват информации путем внедрения СВТ электронных устройств перехвата информации.
32	Пассивные методы защиты акустической (речевой) информации.
33	Средства и методы защиты информации от утечки по каналам акустоэлектрических преобразований (микрофонный эффект).
34	Активные методы защиты акустической (речевой) информации.
35	Технические каналы утечки видовой информации. Основные определения. Технические характеристики систем видеонаблюдения.
36	Методы и средства поиска закладных электронных устройств перехвата информации. Демаскирующие признаки объектов
37	Общие принципы выявления закладных устройств. Методы поиска закладных устройств как электронных средств

5.2.2 Типовые тестовые задания

не предусмотрены

5.2.3 Типовые практико-ориентированные задания (задачи, кейсы)

1. Нарисуйте спектр периодического аналогового сигнала.
2. Нарисуйте осциллограмму бинарного сигнала
3. Нарисуйте спектр бинарного сигнала
4. Рассчитайте оптимальное количество датчиков пожарной безопасности в офисном помещении площадью 56 кв.м. с главным и черным входом и тремя окнами стандартного размера.
5. Рассчитайте оптимальное количество датчиков пожарной безопасности в офисном помещении площадью 48 кв.м. с единственным входом и двумя окнами стандартного размера.
6. Рассчитайте оптимальное количество видеокамер в складском помещении площадью 168 кв.м. с высотой потолков 4.5 м и наличием 2 ворот и 4 входов

5.3 Методические материалы, определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности)

5.3.1 Условия допуска обучающегося к промежуточной аттестации и порядок ликвидации академической задолженности

Проведение промежуточной аттестации регламентировано локальным нормативным актом СПбГУПТД «Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся»

5.3.2 Форма проведения промежуточной аттестации по дисциплине

Устная + Письменная Компьютерное тестирование Иная

5.3.3 Особенности проведения промежуточной аттестации по дисциплине

Обучающийся тянет билет, в котором два теоретических вопроса и практическое задание. После этого готовится в течении 30 минут. Обучающийся в устной форме доводит до преподавателя ответ на вопрос, при необходимости прямо во время ответа составляет необходимые схемы или диаграммы. После ответа на теоретические вопросы обучающийся приступает к решению практического задания, гарантированно на решение задачи времени дается 10 минут.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная учебная литература				
Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование	2019	http://www.iprbookshop.ru/87995.html
Жук А.П., Жук Е.П., Лепешкин О.М. и др.	Защита информации	Москва: ИЦ РИО	2021	https://ibooks.ru/reading.php?short=1&productid=361250
6.1.2 Дополнительная учебная литература				
Фомин, Д. В.	Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства	Саратов: Вузовское образование	2018	http://www.iprbookshop.ru/77317.html
Шипов, О. В.	Пожарная безопасность объектов защиты	Тюмень: Государственный аграрный университет Северного Зауралья	2021	https://www.iprbookshop.ru/117672.html
Ворожейкин, В. Н.	Технические средства и методы защиты информации – дополнительные главы	Самара: Самарский государственный технический университет, ЭБС АСВ	2019	https://www.iprbookshop.ru/111432.html

6.2 Перечень профессиональных баз данных и информационно-справочных систем

1. Информационно-справочная система «Консультант Плюс» [Электронный ресурс] // Режим доступа:<http://www.consultant.ru/>
2. Научная электронная библиотека [Электронный ресурс] // Режим доступа:<https://elibrary.ru/>
3. Справочно-правовая система «Гарант»[Электронный ресурс] // Режим доступа: <http://www.garant.ru/>
4. Электронная библиотека диссертаций [Электронный ресурс] // Режим доступа:<http://diss.rsl.ru/>
5. Официальный сайт ФСТЭК России[Электронный ресурс] // Режим доступа: <http://www.fstec.ru>
6. Банк данных угроз безопасности информации ФСТЭК России[Электронный ресурс] // Режим доступа: <https://bdu.fstec.ru/>
7. Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 [Электронный ресурс] // Режим доступа: <https://reestrinform.ru/reestr-szi.html>
8. ГОСТ Эксперт - единая база ГОСТов Российской Федерации [Электронный ресурс] // Режим доступа:<https://gostexpert.ru/>

6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

MicrosoftOfficeProfessional

Microsoft Windows

6.4 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Аудитория	Оснащение
Компьютерный класс	Специализированная мебель; компьютерная техника; наборы демонстрационного оборудования, служащие для представления учебной информации (стационарное мультимедийное оборудование) - мультимедийная проекционная система (мультимедиа проектор и экран). Рабочие станции, программно-аппаратные комплексы ЗИ; локальная вычислительная сеть с выходом в Интернет, система «Шепот». Многофункциональный поисковый прибор ST 031M "Пиранья". СЗИ НСД «Аккорд-АМДЗ». Универсальный досмотровый набор.