Документ подписан простой электронной подписью
Информация о владельце:
ФИО: ПАНОВ Юрий Петрович
Должность: Ректор
Дата подписания: 09.06.2025 11:34:26
Уникальный программный ключ:
e30ba4f0895d1683ed43800960e77389e6cbff62

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Российский государственный геологоразведочный университет имени Серго Орджоникидзе"

(МГРИ)

СПЕЦИАЛИЗАЦИЯ
Кодирование информации в автоматизированных системах управления

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Автоматизации, роботизации и искусственного интеллекта**

Учебный план s100503_25_BZO25.plx
Специальность 10.05.03 Информационная безопасность автоматизированных систем

Квалификация **Специалист по защите информации**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану	144	Виды контроля в семестрах:
в том числе:		зачеты с оценкой 10
аудиторные занятия	56,25	
самостоятельная работа	87,75	

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**10 (5.2)**		Итого	
Недель	14 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	28	28	28	28
Практические	28	28	28	28
Иные виды контактной работы	0,25	0,25	0,25	0,25
В том числе инт.	4	4	4	4
Итого ауд.	56,25	56,25	56,25	56,25
Контактная работа	56,25	56,25	56,25	56,25
Сам. работа	87,75	87,75	87,75	87,75
Итого	144	144	144	144

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины является теоретическая и практическая подготовка к деятельности, связанной с применением основных знаний, умений и навыков в области теории информации, необходимых специалисту по радиоэлектронным системам и комплексам.
1.2	Задачи дисциплины:
1.3	изучение базовых понятий теории информации; изучение математических моделей дискретных источников информации и каналов связи;
1.4	изучение методов кодирования дискретных источников информации;
1.5	изучение методов помехоустойчивого кодирования для дискретных каналов связи без памяти; овладение навыками применения методов теории информации в области информационной безопасности автоматизированных систем.
1.6	Автоматизированные системы управления

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В.10
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Практикум по решению научно-исследовательских задач профессиональной деятельности
2.1.2	Цифровая обработка сигналов в системах обеспечения информационной безопасности автоматизированных систем управления
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-1: Способен моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации	
Знать:	
Уровень 1	методы проведения физических исследований, технические и программные средства, применяемые при анализе электромагнитных полей и волн; уравнения и законы электродинамики и распространения радиоволн; модели элементарных излучателей; основные типы антенн, применяемых при анализе электромагнитных полей; принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов;
Уровень 2	назначение, функции и структуру информационных и библиографических систем; методы поиска, изучения и обобщения научно-технической литературы, нормативных и методических материалов; основные методы исследования по теме своей научно- исследовательской работы; основы теории цифровой обработки сигналов как теоретической базы для разработки и исследования методов обработки, приема и передачи данных в системах обеспечения информационной безопасности автоматизированных систем управления; актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности; цели и задачи автоматизации управления, общие понятия автоматизированных систем управления (АСУ), жизненный цикл, функции и виды АСУ
Уровень 3	состав автоматизированных систем управления технологическим процессом (АСУ ТП), виды обеспечения, классификацию и уровни управления АСУ ТП, место АСУ ТП в интегрированных системах управления; области задач организации информационных технологий и современные инструменты построения интеллектуальных систем, обеспечивающих информационную безопасность; основные принципы и проблематику теории обучения машин, основные современные методы обучении по прецедентам — классификации, кластеризации и регрессии; принципы организации информационных систем в соответствии с требованиями по защите информации; основные способы кодирования информации в автоматизированных системах управления (АСУ), обеспечивающие максимальную надежность и высокую скорость при ее передаче по каналам связи (коды: линейные, циклические, БЧХ, Хэмминга, Шеннона - Фано и Хаффмана); уязвимости современных АСУ ТП, подходы к устранению уязвимостей и построению системы защиты современных АСУ ТП; основные виды математических моделей информационных потоков и систем защиты информации и методы их построения
Уметь:	
Уровень 1	использовать методы проведения физических исследований, технические и программные средства для анализа электромагнитных полей технических средств автоматизированных систем; использовать методы исследования электромагнитных полей для оценки физических характеристик технических средств автоматизированных систем;

	определять типы субъектов доступа и объектов доступа, являющихся объектами защиты; определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе; определять параметры информационной системы и ее структуру в соответствии с заданными функциями
Уровень 2	составлять обзоры по вопросам обеспечения информационной безопасности по теме своей научно-исследовательской работы; применять методы исследования по теме своей научно-исследовательской работы; формировать математическое описание дискретных систем в виде алгоритмов; выполнять компьютерное моделирование дискретных систем на основе их математического описания; анализировать и оценивать риски информационной безопасности в промышленных и корпоративных системах автоматизации; анализировать и моделировать информационные процессы, протекающие в системах промышленной автоматизации; формулировать основные задачи, возникающие при анализе данных, пути их решения, выбирать адекватные алгоритмы решения задачи анализа данных, оценивать качество получаемых решений, обеспечивающих информационную безопасность;
Уровень 3	формализовать постановки прикладных задач анализа данных, применять основные методы создания алгоритмов интеллектуального анализа данных в системах информационной безопасности, такие как классификация, кластеризация и прогнозирование; оценивать информационные риски в информационных системах; решать типовые задачи кодирования и декодирования информации с использованием математических методов и моделей; анализировать структуры АСУ ТП, строить их модели, оценивать риски функциональной безопасности, распознавать атаки социальной инженерии; на основе опытных данных и технических характеристик автоматизированной системы управления (АСУ) строить адекватную математическую модель, связанную с системой защиты информации в АСУ
Владеть:	
Уровень 1	навыком применения методик исследования электромагнитных полей; навыком применения исследовательских методов электродинамики и распространения радиоволн; навыками поиска и изучения научно-технической литературы, а также изложения и оформления результатов своей научно-исследовательской работы; навыком составления математических моделей дискретных систем и сигналов;
Уровень 2	навыком разработки алгоритмов цифровой обработки сигналов в системах информационной безопасности; навыком выбора методов проведения и обработки экспериментальных исследований, оформления научно-технических отчётов, обзоров, докладов, статей; навыком выбора и обоснованием критериев эффективности функционирования защищенных информационных систем
Уровень 3	навыком применения помехоустойчивых шифров и кодов, повышающих скорость передачи информации в АСУ; навыком разработки политик безопасности современных промышленных систем автоматизации, исследования сетевых пакетов в промышленной сети; навыком применения математических моделей для построения системы защиты информации в АСУ и оценки ее эффективности

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	цели и задачи автоматизации управления, общие понятия автоматизированных систем управления (АСУ), жизненный цикл, функции и
3.1.2	виды АСУ;
3.1.3	состав автоматизированных систем управления технологическим процессом (АСУ ТП), виды обеспечения, классификацию и
3.1.4	уровни управления АСУ ТП, место АСУ ТП в интегрированных системах управления, архитектуру промышленных сетей АСУ ТП;
3.1.5	актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как
3.1.6	ответную реакцию на внедрение средств и мер информационной безопасности, типы современных киберугроз в промышленных и
3.1.7	корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП;
3.1.8	средства и меры информационной
3.1.9	безопасности, применяемые в промышленных и корпоративных системах автоматизации
3.2	**Уметь:**

3.2.1	анализировать и моделировать информационные процессы, протекающие в системах промышленной автоматизации, применять методы и средства регистрации, записи и хранения значимых параметров потоков данных АСУ ТП;
3.2.2	анализировать и оценивать риски информационной безопасности в промышленных и корпоративных системах автоматизации, проводить аналитику современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП
3.3	**Владеть:**
3.3.1	определения ключевых точек мониторинга значимых параметров потоков данных, распределенных в информационной системе промышленных сетей АСУ ТП;
3.3.2	идентификации и моделирования каналов возможного деструктивного информационно-технического воздействия в промышленных и
3.3.3	корпоративных системах автоматизации, оценки уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Особенности информационных каналов в автоматизированных системах управления						
1.1	Введение. Понятие информации. Основные соглашения относительно представления информации. /Лек/	10	1	ПК-1	Л1.1 Л1.2Л2.1	0	
1.2	Информационные каналы в автоматизированных системах управления и их особенности /Лек/	10	1	ПК-1	Л1.1 Л1.2Л2.1	0	
	Раздел 2. Дискретные источники. Кодирование дискретных источников						
2.1	Математическая модель источника сообщений. Примеры источников сообщения. Стационарные источники. /Лек/	10	1	ПК-1	Л1.1 Л1.2Л2.1	0	
2.2	Алфавитное кодирование. Однозначно декодируемые, префиксные и суффиксные коды. Алгоритмы Фано и Хаффмана. Леммы о строении оптимального кода. Теорема об оптимальности двоичного кода Хаффмана. /Лек/	10	1	ПК-1	Л1.1 Л1.2Л2.1	0	
2.3	Префиксные коды. К-ичное дерево и его связь с префиксными кодами /Пр/	10	4	ПК-1	Л1.1 Л1.2Л2.1	0	
2.4	Префиксные коды Коды Шеннона-Фано и Хаффмана. /Пр/	10	4	ПК-1	Л1.1 Л1.2Л2.1	1	
2.5	Контрольная работа по теме "Коды, минимизирующие длину сообщения" /Пр/	10	4	ПК-1	Л1.1 Л1.2Л2.1	1	
2.6	Декодирование специальных кодов /Ср/	10	22,75	ПК-1	Л1.1 Л1.2Л2.1	0	
2.7	Подготовка к практическим занятиям. Выполнение домашних заданий /Ср/	10	21	ПК-1	Л1.1 Л1.2Л2.1	0	
	Раздел 3. Дискретные каналы связи						

3.1	Математическая модель канала связи и его информационные характеристики. Дискретный стационарный канал без памяти (ДКБП). Определение пропускной способности. Симметричные каналы связи. Утверждения о пропускной способности симметричных каналов. /Лек/	10	2	ПК-1	Л1.1 Л1.2Л2.1	0	
3.2	Теоремы кодирования для дискретных каналов без памяти /Лек/	10	2	ПК-1	Л1.1 Л1.2Л2.1	0	
3.3	Исследование характеристик линейного кода /Ср/	10	22	ПК-1	Л1.1 Л1.2Л2.1	0	
	Раздел 4. Помехоустойчивые коды						
4.1	Примеры помехоустойчивых кодов. Линейное кодирование и линейный код. Порождающая и проверочная матрица линейного кода. /Лек/	10	2	ПК-1	Л1.1 Л1.2Л2.1	0	
4.2	Коды обнаруживающие и исправляющие ошибки. Расстояние Хэмминга. Декодирование по принципу максимальной вероятности и в «ближайшего соседа». Минимальное расстояние кода как характеристика его надежности. /Лек/	10	2	ПК-1	Л1.1 Л1.2Л2.1	0	
4.3	Двойственный код и его характеристики. /Лек/	10	2	ПК-1	Л1.1 Л1.2Л2.1	0	
4.4	Декодирование с помощью синдромов и лидеров. /Лек/	10	2	ПК-1	Л1.1 Л1.2Л2.1	0	
4.5	Границы для минимального расстояния кода. Совершенные коды. /Лек/	10	2	ПК-1	Л1.1 Л1.2Л2.1	0	
4.6	Циклические коды. Порождающие и проверочный многочлены циклического кода, их свойства. Связь порождающего и проверочного многочленов циклического кода с порождающей и проверочной матрицами. Алгоритмы кодирования и декодирования для циклического кода. /Лек/	10	2	ПК-1	Л1.1 Л1.2Л2.1	0	
4.7	Коды Хэмминга и их характеристики /Лек/	10	2	ПК-1	Л1.1 Л1.2Л2.1	0	
4.8	Бинарный симплексный код и его характеристики /Лек/	10	2	ПК-1	Л1.1 Л1.2Л2.1	0	
4.9	БЧХ-коды и их характеристики /Лек/	10	2	ПК-1	Л1.1 Л1.2Л2.1	0	
4.10	Коды Рида-Маллера. Декодирование кодов Рида - Маллера /Лек/	10	2	ПК-1	Л1.1 Л1.2Л2.1	0	
4.11	Линейное кодирование и линейный код. Порождающая и проверочная матрица линейного кода Минимальное расстояние кода и способы его определения Декодирование с помощью таблицы синдромов и лидеров /Пр/	10	2	ПК-1	Л1.1 Л1.2Л2.1	0	
4.12	Контрольная работа "Общие характеристики кодов" /Пр/	10	2	ПК-1	Л1.1 Л1.2Л2.1	0	
4.13	Коды Хэмминга. Бинарный симплексный код /Пр/	10	2	ПК-1	Л1.1 Л1.2Л2.1	0	

4.14	Коды Рида -Маллера. БЧХ-коды /Пр/	10	4	ПК-1	Л1.1 Л1.2Л2.1	1	
4.15	Циклические коды и их характеристики /Пр/	10	4	ПК-1	Л1.1 Л1.2Л2.1	0	
4.16	Контрольная работа "Специальные линейные коды" /Пр/	10	2	ПК-1	Л1.1 Л1.2Л2.1	1	
4.17	Построение кодов Шеннона-Фано и Хаффмана /Ср/	10	22	ПК-1	Л1.1 Л1.2Л2.1	0	
4.18	Зачет /ИВКР/	10	0,25	ПК-1	Л1.1 Л1.2Л2.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

1. Что такое информация и каково её значение в технических системах?
2. Какие существуют подходы к определению информации?
3. Какие основные соглашения приняты при представлении информации в технических системах?
4. Что такое информационные каналы и какова их роль в автоматизированных системах управления?
5. Какими особенностями обладают информационные каналы в АСУ?
6. Что такое математическая модель источника сообщений?
7. Какие существуют примеры источников сообщений?
8. Что означает понятие "стационарный источник сообщений"?
9. Каковы свойства стационарных источников?
10. Что такое алфавитное кодирование?
11. Какие требования предъявляются к однозначно декодируемым кодам?
12. Чем отличаются префиксные коды от других типов кодов?
13. Что представляют собой суффиксные коды и как они используются?
14. В чем суть алгоритма Фано?
15. Как работает алгоритм Хаффмана?
16. Что утверждают леммы о строении оптимального кода?
17. Как формулируется теорема об оптимальности двоичного кода Хаффмана?
18. Что такое математическая модель канала связи?
19. Какие характеристики определяют информационную способность канала?
20. Что представляет собой дискретный стационарный канал без памяти?
21. Как определяется пропускная способность канала?
22. Что такое симметричный канал и чем он отличается от других?
23. Какова пропускная способность симметричного канала?
24. Что утверждают теоремы кодирования для ДКБП?
25. Какие существуют примеры помехоустойчивых кодов?
26. Что такое линейное кодирование?
27. Что представляет собой линейный код?
28. Какова роль порождающей матрицы в линейном кодировании?
29. Для чего используется проверочная матрица?
30. Что такое коды, обнаруживающие ошибки?
31. Как устроены коды, исправляющие ошибки?
32. Что такое расстояние Хэмминга?
33. Почему расстояние Хэмминга важно в кодировании?
34. Как работает декодирование по принципу максимальной вероятности?
35. Что означает декодирование по принципу ближайшего соседа?
36. Как минимальное расстояние кода влияет на его надежность?
37. Что такое двойственный код?
38. Какие характеристики имеет двойственный код?
39. Что такое синдром и как он используется при декодировании?
40. Кто такие лидеры в контексте синдромного декодирования?
41. Какие существуют границы для минимального расстояния кода?
42. Что такое совершенный код?
43. Какие условия должны выполняться для существования совершенного кода?
44. Как связаны между собой параметры кода: длина, мощность и минимальное расстояние?
45. Какие типы ошибок чаще всего встречаются в цифровых каналах связи?
46. Как осуществляется построение кода по заданной проверочной матрице?
47. Какие методы используются для построения порождающей матрицы?
48. Что означает "линейность" кода в контексте теории кодирования?
49. Как классифицируются дискретные каналы связи по памяти?
50. Какие существуют методы оценки эффективности кодирования?
51. Каков смысл вероятности ошибки декодирования и как её минимизировать?
52. Почему префиксные коды считаются удобными для практической реализации?

53. В чем преимущества алгоритма Хаффмана перед другими методами кодирования?
54. Как обеспечить устойчивость передачи информации в условиях помех?
55. Что такое энтропия источника сообщений и как она рассчитывается?
56. Как энтропия источника влияет на выбор оптимального кода?
57. Почему не все коды могут быть однозначно декодируемыми?
58. Каково значение понятия "избыточность кода"?
59. Какие компромиссы существуют между длиной кода и его надежностью?
60. Что означает "эффективность кода"?
61. Как код Хаффмана обеспечивает минимальную среднюю длину кодового слова?
62. Что такое система кодов с фиксированной и переменной длиной?
63. Как можно визуализировать структуру префиксных кодов?
64. Какие практические применения имеют коды с исправлением ошибок?
65. Каковы области применения линейных кодов?
66. Чем отличаются коды Хэмминга от других кодов?
67. Как строится код Хэмминга и как он исправляет ошибки?
68. Что означает "кодовое пространство" в теории кодирования?
69. Как определяются вес и расстояние в кодовом пространстве?
70. Какова роль матрицы Парити в проверке целостности данных?
71. Что такое избыточные биты и зачем они нужны в кодировании?
72. Как осуществляется автоматическое исправление одиночных ошибок?
73. Какие математические основы лежат в построении кодов Рида-Соломона?
74. Что такое циклический код и где он применяется?
75. В чем преимущества использования синдромного декодирования?
76. Как выбирать оптимальный код для конкретного канала передачи?
77. Как анализировать производительность кодов при различных уровнях помех?
78. Что означает кодирование с контролем чётности?
79. Как рассчитать вероятность ошибки при передаче через канал?
80. Какие существуют методы проверки корректности декодированных сообщений?
81. Как связаны понятия алфавита, кодовых слов и мощности кода?
82. В чем суть концепции избыточности информации и её роли в надёжности связи?
83. Какие примеры практического применения теории информации вы знаете?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Кодирование информации в автоматизированных системах управления" обеспечена оценочными средствами для проведения текущего контроля и промежуточной аттестации, включающими контрольные вопросы для проведения промежуточной аттестации, критерии оценивания учебной деятельности обучающихся по балльно-рейтинговой системе, примеры заданий для практических и лабораторных занятий, билеты для проведения промежуточной аттестации.
Все оценочные средства представлены в Приложении 1.

5.4. Перечень видов оценочных средств

Оценочные средства разработаны для всех видов учебной деятельности студента - лекций, практических занятий, самостоятельной работы и промежуточной аттестации. Оценочные средства представлены в виде:
- средства текущего контроля: проверочных работ по решению задач, дискуссии по теме;
- средств итогового контроля - промежуточной аттестации: экзамена в 10 семестре.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Седякин В. П.	Теория информации: учебник для вузов	Санкт-Петербург: Лань, 2024
Л1.2	Осокин А. Н., Мальчуков А. Н.	Теория информации: учебное пособие для вузов	Москва: Юрайт, 2024

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Рахимов Р. З., Рахимова Н. Р.	История науки и техники	Санкт-Петербург: Лань, 2022

6.3.1 Перечень программного обеспечения

6.3.1.1	Office Professional Plus 2019	
6.3.1.2	Windows 10	

6.3.1.3	МТС-Линк	Комплексная платформа для коммуникаций, обучения и совместной работы, разработанная с использованием современных технологий. Доступны десктопные и мобильные приложения для удобной работы с системой.
6.3.2 Перечень информационных справочных систем		
6.3.2.1	База данных научных электронных журналов "eLibrary"	
6.3.2.2	Электронно-библиотечная система "Лань" Доступ к коллекциям электронных изданий ЭБС "Издательство "Лань"	
6.3.2.3	Электронно-библиотечная система «Книжный Дом Университета» ("БиблиоТех")	

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение	Вид
1	Специализированная многофункциональная учебная аудитория № 1 для проведения учебных занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной/ итоговой аттестации	Столы обучающихся; Стулья обучающихся; Письменный стол педагогического работника; Стул педагогического работника; Кафедра; Магнитно-маркерная доска; Мультимедийный проектор; Экран; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	
5	Помещение № 5 для самостоятельной работы обучающихся	Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде	

6-25	Специализированная многофункциональная лаборатория № 6-25 для проведения практических и лабораторных занятий, текущего контроля и промежуточной/ итоговой аттестации, в том числе для организации практической подготовки обучающихся	Компьютерные столы; Стулья; Письменный стол педагогического работника; Стул педагогического работника; Магнитно-маркерная доска; Мультимедийный проектор; Экран; ПК с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Телекоммуникационные шкафы; Средства отображения информации. Стенды сетей передачи информации с коммутацией пакетов и коммутацией каналов в составе: Учебный стенд "Основы IP-сетей" (маршрутизаторы, коммутаторы L2/L3); Учебный стенд "Виртуальные сети (VLAN, VPN)"; Учебный стенд "Беспроводные сети (Wi-Fi, IoT)"; Учебный стенд "Телефония (ISDN, VoIP)"; Учебный стенд "Оптические сети (PON, DWDM)"; Стенд "Цифровые системы передачи (E1, SDH)". Стенды для изучения проводных и беспроводных компьютерных сетей в составе: абонентские устройства; коммутаторы; маршрутизаторы; точкидоступа, межсетевые экраны; средства обнаружения компьютерных атак; системы углубленной проверки сетевых пакетов; системы защиты от утечки данных; анализаторы кабельных сетей. Учебно-лабораторные комплексы в составе: Учебный лабораторный комплекс контроля сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры). Учебный лабораторный комплекс проведения анализа защищенности значимого объекта КИИ на соответствие	

		требованиям по обеспечению безопасности. Учебный лабораторный комплекс для обеспечения исследований специального программного обеспечения и аппаратного СЗИ в составе: средства защиты информации от НСД; программно-аппаратный комплекс доверенной нагрузки; антивирусные программные комплексы; межсетевые экраны; средства создания модели разграничения доступа; программа контроля полномочий доступа к информационным ресурсам; программа фиксации и контроля исходного состояния программного комплекса; программа поиска и гарантированного уничтожения информации на дисках; аппаратные средства аутентификации пользователя; системы обнаружения вторжений и анализа защищенности; средства анализа защищенности компьютерных сетей; сканеры безопасности; устройства чтения смарт-карт и радиометок; программно-аппаратные комплексы защиты информации; средства криптографической защиты информации. Учебный лабораторный комплекс для обеспечения исследований типовых сертифицированных программных и программно-технических средств защиты информации от НСД. Учебный лабораторный комплекс для обеспечения исследований сертифицированных средств в которых реализованы средства защиты информации от НСД. УЛК для проведения аттестационных испытаний автоматизированных систем от НСД по требованиям безопасности информации. Аппаратно-программные комплексы в составе: аппаратно-программные средства управления	

		доступом к данным; средства криптографической защиты информации; средства дублирования и восстановления данных; средства мониторинга состояния автоматизированных систем; средства контроля и управления доступом в помещения.	
Ауд. 8	Аудитория для научно-исследовательской работы обучающихся, курсового и дипломного проектирования № 8	Рабочие места на базе вычислительной техники с набором необходимых для проведения и оформления результатов исследований дополнительных аппаратных и/или программных средств; Письменный стол обучающегося; Стул обучающегося; Письменный стол обучающегося с ограниченными возможностями здоровья; Стул обучающегося с ограниченными возможностями здоровья; Ноутбук с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде лицензиата; Моноблок (в том числе, клавиатура, мышь, наушники) с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде; Многофункциональное устройство (принтер, сканер, ксерокс).	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по изучению дисциплины "Кодирование информации в автоматизированных системах управления" представлены в Приложении 2 и включают в себя:
1. Методические указания для обучающихся по организации учебной деятельности.
2. Методические указания по организации самостоятельной работы обучающихся.
3. Методические указания по организации процедуры оценивания знания, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.