МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Кибербезопасность интеллектуальных автоматизированных систем управления технологическими процессами

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Промышленной кибербезопасности и защиты геоданных**

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:		экзамены 10
аудиторные занятия	86,35	
самостоятельная работа	30,65	
часов на контроль	27	

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
Лабораторные	28	28	28	28
Практические	28	28	28	28
Иные виды контактной работы	2,35	2,35	2,35	2,35
В том числе инт.	8	8	8	8
Итого ауд.	86,35	86,35	86,35	86,35
Контактная работа	86,35	86,35	86,35	86,35
Сам. работа	30,65	30,65	30,65	30,65
Часы на контроль	27	27	27	27
Итого	144	144	144	144

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины является приобретение знаний о проблемах обеспечения кибербезопасности в критических системах и навыков, которые необходимы при работе по обеспечению информационной безопасности АСУ ТП на критических объектах.
1.2	Дисциплина включает материалы, лежащие на стыке двух отраслей: информационная безопасность и автоматизация производств.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Защита информации в сети Интернет
2.1.2	Автоматизированные системы управления
2.1.3	Современные киберугрозы в промышленных и корпоративных системах автоматизации
2.1.4	Производственная практика (научно-исследовательская работа)
2.1.5	Практикум по решению научно-исследовательских задач профессиональной деятельности
2.1.6	Биометрические технологии контроля доступа
2.1.7	Практикум по решению эксплуатационных задач профессиональной деятельности
2.1.8	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

ПК-4: Способен разрабатывать организационно-распорядительные документы и внедрять организационные меры по защите информации в автоматизированных системах	
Знать:	
Уровень 1	правовые основы организации защиты государственной тайны и/или конфиденциальной информации; задачи органов защиты государственной тайны и/или служб защиты информации на предприятии; свойства, функции и признаки документа, в том числе как объекта нападения и защиты; основы документационного обеспечения управления;
Уровень 2	задачи органов защиты информации на предприятиях; действующие нормативные и методические документы по оформлению рабочей технической документации; понятие и виды террористической деятельности, основы государственной политики Российской Федерации по противодействию терроризму в информационной сфере; нормативно-методические и руководящие документы, регламентирующие обеспечение информационной безопасности значимых объектов критической информационной инфраструктуры;
Уровень 3	категории и характеристики значимых объектов критической информационной инфраструктуры; способы выявления угроз информационной безопасности значимых объектов критической информационной инфраструктуры; нормативные документы Российской федерации в области кибербезопасности; особенности организации подразделения центра управления инцидентами (ЦУИ ИБ) для поддержки информационной безопасности промышленной сети;

	основы правового обеспечения и основные нормативные правовые акты в области защиты информации в различных отраслях деятельности; организацию работы специалистов с документами в автоматизированных системах электронного документооборота
Уметь:	
Уровень 1	анализировать правовые акты и осуществлять правовую оценку информации, циркулирующей в автоматизированной системе; квалифицированно исследовать состав документации предприятия (организации);
Уровень 2	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации; реализовывать с учетом особенностей функционирования систем управления значимых объектов критической информационной инфраструктуры требования нормативно-методической и руководящей документации, а также действующего законодательства по вопросам противодействия террористической деятельности
Уровень 3	разрабатывать предложения по совершенствованию организационно- распорядительных документов по безопасности значимых объектов и представлять их руководителю субъекта критической информационной инфраструктуры (уполномоченному лицу); применять средства юридической защиты информации ограниченного доступа; определять задачи по разработке требований к автоматизированным системам обработки и хранения электронных документов
Владеть:	
Уровень 1	навыком разработки организационно- распорядительных документов по защите информации в автоматизированных системах; навыком формирования требований по защите информации
Уровень 2	навыком применения современной нормативной базы для построения системы организационных и программно -технических мер по выявлению, предупреждению и пресечению террористической деятельности в отношении систем управления значимых объектов критической информационной инфраструктуры
Уровень 3	навыком использования профессиональной терминологии в области защиты информации в различных отраслях деятельности

ПК-5: Способен выполнять работы по администрированию систем защиты информации автоматизированных систем и обеспечивать их работоспособность при возникновении нештатных ситуаций	
Знать:	
Уровень 1	методы и средства контроля и управления доступом при обеспечении безопасности автоматизированных систем; политику безопасности и инструменты администрирования при работе с данными (на рабочих станциях, сервисах, сетях), пользователями, управлением изменениями и обеспечением защищённости и отказоустойчивости администрируемой информационной подсистемы; современные методы предотвращения несанкционированного доступа (НСД) к объектам информатизации, основанные на биометрических технологиях распознавания личности
Уровень 2	принципы организации и структуру систем защиты программного обеспечения автоматизированных систем; средства и способы обеспечения безопасности информации, принципы построения систем защиты информации; принципы формирования политики информационной безопасности автоматизированной системы; основные направления защиты информации в информационно- телекоммуникационных системах в соответствии с законодательством Российской Федерации
Уровень 3	современные технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет; архитектуру автоматизированной системы управления технологическим процессом (АСУ ТП), модели промышленных систем автоматизации, сетевые технологии, используемые в современных АСУ ТП, понятия функциональной и информационной безопасности, их взаимосвязь и противоречия; основы организации своевременной и полноценной обработки инцидентов безопасности
Уметь:	
Уровень 1	использовать устройства контроля и управления доступом при обеспечении безопасности автоматизированных систем; применять политику безопасности и инструменты администрирования при работе с данными (на рабочих станциях, сервисах, сетях), пользователями, управлением изменениями и обеспечением защищённости и отказоустойчивости администрируемой информационной подсистемы; использовать устройства контроля доступа на основе биометрических характеристик человека
Уровень 2	регистрировать события, связанные с защитой информации в автоматизированных системах; проводить комплексное тестирование аппаратных и программных средств; определять комплекс мер (правила, процедуры, практические приёмы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; проводить оценку угроз безопасности информационно- телекоммуникационной системы, подключенной к сети Интернет;

Уровень 3	реализовывать технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет; работать со средствами обеспечения безопасности в системах промышленной автоматизации; настраивать межсетевой экран для обеспечения защиты периметра сети, для обеспечения сегментации внутренней сети
Владеть:	
Уровень 1	навыком использования систем контроля и управления доступом для управления процессами обеспечения безопасности автоматизированных систем; навыком применения инструментов администрирования подсистем информационной безопасности автоматизированной системы; навыком использования специальных средств биометрической идентификации личности для управления процессами обеспечения безопасности автоматизированных систем
Уровень 2	навыком обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы; навыком обеспечения работоспособности автоматизированных систем при возникновении нештатных ситуаций; навыком разработки частных политик информационной безопасности автоматизированных систем
Уровень 3	навыком использования антивирусного программного обеспечения для защиты информации в информационно- телекоммуникационных системах, подключенных к сети Интернет; анализом инцидентов кибербезопасности в современных промышленных системах автоматизации

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	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);
3.1.2	цели и задачи автоматизации управления, общие понятия автоматизированных систем управления (АСУ), жизненный цикл, функции и виды АСУ;состав автоматизированных систем
3.1.3	управления технологическим процессом (АСУ ТП), виды обеспечения, классификацию и уровни управления АСУ ТП, место АСУ ТП в интегрированных системах управления,
3.1.4	архитектуру промышленных сетей АСУ ТП;
3.1.5	актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер
3.1.6	информационной безопасности, типы современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети
3.1.7	АСУ ТП;средства и меры информационной безопасности, применяемые в промышленных и корпоративных системах автоматизации;
3.1.8	основные направления защиты информации в информационно- телекоммуникационных системах в соответствии с законодательством Российской Федерации;современные технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет
3.2	**Уметь:**
3.2.1	решать типовые задачи кодирования и декодирования информации с использованием математических методов и моделей;
3.2.2	анализировать и моделировать информационные процессы, протекающие в системах промышленной автоматизации, применять методы и средства регистрации, записи и хранения значимых параметров потоков данных АСУ ТП;
3.2.3	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;
3.2.4	проводить оценку угроз безопасности информационно-телекоммуникационной системы, подключенной к сети Интернет;реализовывать технологии защиты от вредоносного программного обеспечения, распространяемого по сети Интернет;
3.3	**Владеть:**
3.3.1	применения помехоустойчивых шифров и кодов, повышающих скорость передачи информации в АСУ;
3.3.2	определения ключевых точек мониторинга значимых параметров потоков данных, распределенных в информационной системе промышленных сетей АСУ ТП;
3.3.3	идентификации и моделирования каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных системах автоматизации, оценки уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП;
3.3.4	использования антивирусного программного обеспечения для защиты информации в информационно-телекоммуникационных системах, подключенных к сети Интернет;

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. Введение						
1.1	Эволюция АСУ ТП Технологии современных АСУ ТП /Лек/	10	3	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
1.2	Введение /Ср/	10	3	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
	Раздел 2. Объект исследования – интеллектуальная АСУ ТП						
2.1	Основные определения в области промышленной автоматизации. Модель промышленной системы по ФСТЭК. Модель промышленной системы PERA /Лек/	10	4	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
2.2	Анализ структур различных АСУ ТП /Пр/	10	4	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	1	
2.3	Безопасность сетей АСУ ТП /Ср/	10	3,1	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
	Раздел 3. Функциональная безопасность АСУ ТП						
3.1	Функциональная безопасность в АСУ ТП. Функциональная и информационная безопасность. Их взаимосвязь и противоречие. Дерево сбоев и атак. Единая модель. /Лек/	10	3	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
3.2	Рассмотрение моделей и расчёт рисков функциональной безопасности /Пр/	10	4	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	1	
3.3	Объект исследования – интеллектуальная АСУ ТП /Ср/	10	3,35	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
	Раздел 4. Проблема обеспечения кибербезопасности АСУ ТП						
4.1	Нормативные документы Российской федерации в области кибербезопасности. 31 приказ ФСТЭК и другие документы Федеральный закон 187 Международные нормативные документы. Документы NERC CIP, NIST Понятие эшелонированной защиты. Трудности при внедрении эшелонированной защиты. /Лек/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
4.2	Проблемы обеспечения безопасности современных промышленных систем. Атаки на современные промышленные системы – общие положения. Уязвимости современных промышленных системы – причины. Устранение уязвимостей. Обновление программного обеспечения промышленных систем. Проблемы устранения уязвимостей и способы их решения. Отличительные особенности и проблемы обеспечения методов обеспечения кибербезопасности промышленных предприятий. Угрозы информационной безопасности в АСУ ТП. Объекты защиты АСУ ТП /Лек/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
4.3	Анализ проблем защищённости и выработка требований к защите типовых АСУ ТП /Пр/	10	4	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	1	

4.4	Изучение дампов сетевого трафика промышленных протоколов /Лаб/	10	4	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	1	
4.5	Защита изолированных сетей /Ср/	10	3,3	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
	Раздел 5. Атаки на интеллектуальные АСУ ТП						
5.1	Типовая схема вторжения. Атаки на сети промышленных систем. Сканирование сетевых систем. Средства сканирования сетевых систем. /Лек/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
5.2	Модель атаки и нарушителя АСУ ТП /Пр/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	1	
5.3	Обнаружение и исследование уязвимостей промышленных устройств /Лаб/	10	4	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	1	
5.4	Проблема обеспечения кибербезопасности АСУ ТП /Ср/	10	3,1	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
	Раздел 6. Безопасность сетей АСУ ТП						
6.1	Обзор протоколов сетей АСУ ТП. Принципы работы и вопросы безопасности /Лек/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
6.2	Разбор протоколов сетей АСУ ТП /Пр/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
6.3	Подходы по интеграции в сеть АСУ ТП защитных решений /Пр/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
6.4	Сегментация промышленных сетей /Лаб/	10	4	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	1	
6.5	Настройка IDS для промышленной сети /Лаб/	10	4	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
6.6	Организация подразделения обеспечения промышленной кибербезопасности. Политика безопасности /Ср/	10	3,1	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
	Раздел 7. Защита изолированных сетей						
7.1	Понятие «воздушного зазора». Способы атак на промышленные системы, не подключенные к сети Интернет. Преодоление «воздушного зазора». Сменные носители. Политика использования сменных носителей Атака со стороны поставщиков и внутренних нарушителей. Методы защиты от атак со стороны поставщиков и внутренних нарушителей. /Лек/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
7.2	Угрозы и защита беспроводных коммуникаций в сетях АСУ ТП. Удаленный доступ и его защита. /Лек/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
7.3	Обсуждение проблематики "воздушного зазора" /Пр/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
7.4	Расширенная настройка правил сетевой безопасности для обнаружения целевых атак /Лаб/	10	6	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	1	
7.5	Типовое вредоносное ПО АСУ ТП /Ср/	10	3,2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
	Раздел 8. Социальная инженерия						

8.1	Фишинг с использованием электронной почты. Признаки фишинга. Направленный фишинг. Фишинг с использованием социальных сетей. /Лек/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
8.2	Рассмотрение подходов различных видов социальной инженерии /Пр/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
8.3	Программы повышения осведомлённости сотрудников /Пр/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
8.4	Атаки на интеллектуальные АСУ ТП /Ср/	10	3,3	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
	Раздел 9. Типовое вредоносное ПО АСУ ТП						
9.1	Разбор известных инцидентов атаки промышленных систем посредством вредоносного ПО. /Лек/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
9.2	Обзор типового вредоносного ПО АСУ ТП /Пр/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
9.3	Настройка средств обеспечения ИБ уровня конечного узла /Лаб/	10	6	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
9.4	Функциональная безопасность АСУ ТП /Ср/	10	3	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
	Раздел 10. Организация подразделения обеспечения промышленной кибербезопасности. Политика безопасности						
10.1	Подразделение ИБ АСУ ТП. Особенности организации работы. Задачи подразделения кибербезопасности. Взаимодействие с другими структурами /Лек/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
10.2	Деловая игра по формированию подразделения ИБ АСУ ТП /Пр/	10	2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
10.3	Социальная инженерия /Ср/	10	2,2	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	
10.4	Экзамен /ИВКР/	10	2,35	ПК-1 ПК-4 ПК-5	Л1.1Л2.1	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема 1: Эволюция АСУ ТП. Современные технологии
1. Как развивались системы управления технологическими процессами?
2. Какие этапы развития можно выделить в истории АСУ ТП?
3. Какие современные технологии используются в построении АСУ ТП?
4. Как влияние цифровизации на развитие промышленной автоматизации?
5. В чём отличия традиционных и современных АСУ ТП?

Тема 2: Основные понятия и модели промышленных систем
6. Что такое АСУ ТП и какие её основные компоненты?
7. Какова структура промышленной системы по классификации ФСТЭК?
8. Что представляет собой модель промышленной системы PERA?
9. Какие уровни взаимодействия выделяются в промышленных системах?
10. Какие стандарты описывают архитектуру промышленных сетей?

Тема 3: Функциональная и информационная безопасность
11. Что понимается под функциональной безопасностью в АСУ ТП?
12. Чем отличается функциональная безопасность от информационной?
13. Какие противоречия могут возникать между ними при внедрении?
14. Что такое дерево сбоев и как оно используется в анализе безопасности?
15. Как строится единая модель анализа рисков и угроз в АСУ ТП?

Тема 4: Нормативно-правовая база РФ и международные стандарты
16. Какие федеральные законы регулируют вопросы кибербезопасности в России?
17. Что регламентирует Приказ ФСТЭК №31?
18. Какой смысл несёт Федеральный закон №187-ФЗ?

19. Какие международные стандарты применяются в области ИБ АСУ ТП?
20. Что представляют собой документы NIST, IEC 62443, NERC CIP?
Тема 5: Эшелонированная защита АСУ ТП
21. Что такое эшелонированная защита и как она реализуется?
22. Какие уровни защиты выделяются в промышленных системах?
23. Какие трудности возникают при внедрении зонирования и разделения сетей?
24. Как организуется защита между различными уровнями АСУ ТП?
25. Как обеспечивается межсетевой экран между IT и OT-средами?
Тема 6: Угрозы и уязвимости в АСУ ТП
26. Какие типичные угрозы существуют для промышленных систем?
27. Почему уязвимы устаревшие протоколы промышленных сетей?
28. Какие последствия может иметь атака на систему SCADA?
29. Какие причины возникновения уязвимостей в промышленных системах?
30. Какие проблемы возникают при обновлении программного обеспечения АСУ ТП?
Тема 7: Особенности обеспечения кибербезопасности промышленных предприятий
31. Чем отличаются подходы к защите промышленных и офисных сетей?
32. Какие объекты требуют особого внимания в АСУ ТП?
33. Какие ограничения накладывает надёжность оборудования на обеспечение безопасности?
34. Как влияет необходимость бесперебойной работы на выбор методов защиты?
35. Как организовать защиту в условиях ограниченной совместимости?
Тема 8: Сценарии вторжения и сетевые атаки
36. Какие типичные сценарии вторжения в промышленные сети?
37. Как осуществляется сканирование и разведка в промышленных сетях?
38. Какие инструменты используются злоумышленниками для аудита сетей?
39. Какие протоколы наиболее уязвимы в промышленных сетях?
40. Как происходит эксплуатация уязвимостей протоколов Modbus, DNP3 и других?
Тема 9: Атаки на "воздушный зазор"
41. Что такое «воздушный зазор» и как он применяется в промышленности?
42. Какие способы преодоления воздушного зазора известны?
43. Как USB-носители могут использоваться для передачи вредоносного кода?
44. Какие политики использования сменных носителей рекомендованы?
45. Как предотвратить атаки через сторонних поставщиков и внутренних пользователей?
Тема 10: Беспроводные коммуникации и удалённый доступ
46. Какие беспроводные технологии используются в промышленных системах?
47. Какие угрозы связаны с использованием Wi-Fi и ZigBee в АСУ ТП?
48. Как организовать безопасный удалённый доступ к системам управления?
49. Какие протоколы обеспечивают безопасность удалённого доступа?
50. Какие меры применяются для защиты от несанкционированного доступа через удалённые точки?
Тема 11: Социальная инженерия и фишинг
51. Какие виды социальной инженерии распространены в промышленных средах?
52. Что такое фишинг и как он реализуется через электронную почту?
53. Чем отличается направленный фишинг от массового?
54. Как злоумышленники используют социальные сети для атаки на сотрудников?
55. Какие меры повышают устойчивость персонала к атакам социальной инженерии?
Тема 12: Известные инциденты и атаки на АСУ ТП
56. Какие известные случаи атак на промышленные системы произошли?
57. Что собой представляет Stuxnet и как он работал?
58. Как происходила атака BlackEnergy на энергетические объекты Украины?
59. Какие уроки извлеклись после инцидента TRITON?
60. Какие выводы сделаны после анализа реальных кибератак на критическую инфраструктуру?
Тема 13: Организация службы информационной безопасности
61. Как организуется подразделение по защите АСУ ТП в крупной организации?
62. Какие задачи выполняет служба кибербезопасности в промышленной среде?
63. Как строится взаимодействие между ИТ-службой и инженерным персоналом?
64. Какие роли и обязанности должны быть определены в структуре ИБ?
65. Какие метрики эффективности используются для оценки деятельности подразделения?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Кибербезопасность интеллектуальных автоматизированных систем управления технологическими процессами" 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	Трофимов В. В., Барабанова М. И., Кияев В. И.	Глобальные и локальные сети: учебник для вузов	Москва: Юрайт, 2024

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Музипов Х. Н., Кузяков О. Н., Хохрин С. А., Чащина М. В., Мартынюк Р. В.	Интегрированные системы проектирования и управления. SCADA	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	Лаб

		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 "Кибербезопасность интеллектуальных автоматизированных систем управления технологическими процессами" 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.