МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

(МГРИ)

Современные киберугрозы в промышленных и корпоративных системах автоматизации

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 **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 48,25
самостоятельная работа 59,75

Виды контроля в семестрах:
зачеты 9

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**9 (5.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	16	16	16	16
Иные виды контактной работы	0,25	0,25	0,25	0,25
В том числе инт.	4	4	4	4
Итого ауд.	48,25	48,25	48,25	48,25
Контактная работа	48,25	48,25	48,25	48,25
Сам. работа	59,75	59,75	59,75	59,75
Итого	108	108	108	108

Москва 2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Изучение основ киберугроз в промышленных и корпоративных системах автоматизации.
1.2	Изучение методов и подходов к оценке киберугроз в промышленных и корпоративных системах автоматизации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Практикум по решению научно-исследовательских задач профессиональной деятельности
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Кибербезопасность интеллектуальных автоматизированных систем управления технологическими процессами
2.2.2	Кодирование информации в автоматизированных системах управления
2.2.3	Мониторинг информационной безопасности автоматизированных систем управления
2.2.4	Математическое моделирование информационных потоков и систем защиты информации

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-3: Способен выполнять работы по мониторингу и аудиту защищенности информации в автоматизированных системах	
Знать:	
Уровень 1	архитектуру промышленных сетей АСУ ТП; физические принципы, на которых строятся системы инженерно-технической защиты объектов; типы современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП;
Уровень 2	средства и меры информационной безопасности, применяемые в промышленных и корпоративных системах автоматизации; основные понятия мониторинга событий, методы сбора информации о событиях, принципы работы систем управления информацией и событиями в безопасности SIEM;
Уровень 3	принципы работы систем мониторинга информационной безопасности автоматизированных систем; методы и средства обеспечения информационной безопасности в системах электронного документооборота;
Уметь:	
Уровень 1	применять методы и средства регистрации, записи и хранения значимых параметров потоков данных АСУ ТП; проводить оптимизацию структуры комплексов инженерно-технической защиты объектов;
Уровень 2	проводить аналитику современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП; использовать средства сбора и анализа информации о событиях информационной безопасности для целей мониторинга информационной безопасности;
Уровень 3	формировать правила анализа событий мониторинга информационной безопасности автоматизированных систем; определять необходимые методы и средства обеспечения информационной безопасности в системах электронного документооборота;
Владеть:	
Уровень 1	навыком определения ключевых точек мониторинга значимых параметров потоков данных, распределенных

	в информационной системе промышленных сетей АСУ ТП; навыком анализа критериев оценки параметров технических средств охраны объектов;
Уровень 2	навыком составления программы испытаний систем инженерно- технической защиты объектов; навыком оценки уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП;
Уровень 3	навыком использования методов мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; навыком проведения контрольных проверок работоспособности и эффективности применяемых программно -аппаратных, криптографических и технических средств защиты информации;

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.2	**Уметь:**
3.3	**Владеть:**

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. Основные понятия и определения. Киберугрозы в промышленных и корпоративных системах автоматизации						
1.1	Актуальные угрозы информационной безопасности промышленных компаний, текущее состояние и эволюцию киберугроз как ответную реакцию на внедрение средств и мер информационной безопасности /Лек/	9	6	ПК-1 ПК-3	Л1.1 Л1.2	0	
1.2	Типы современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП; средства и меры информационной безопасности, применяемые в промышленных и корпоративных системах автоматизации /Лек/	9	6	ПК-1 ПК-3	Л1.1 Л1.2	0	
1.3	Идентификация и моделирование каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных системах автоматизации /Лек/	9	4	ПК-1 ПК-3	Л1.1 Л1.2	0	
1.4	Идентификация каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных системах автоматизации /Пр/	9	4	ПК-1 ПК-3	Л1.1 Л1.2	0	
1.5	Моделирование каналов возможного деструктивного информационно-технического воздействия в промышленных и корпоративных системах автоматизации /Пр/	9	4	ПК-1 ПК-3	Л1.1 Л1.2	4	
1.6	База знаний /Ср/	9	29,95	ПК-1 ПК-3	Л1.1 Л1.2	0	
1.7	Руководство /Ср/	9	29,8	ПК-1 ПК-3	Л1.1 Л1.2	0	
	Раздел 2. Оценка киберугроз в промышленных и корпоративных системах автоматизации						

2.1	Анализ и оценка рисков информационной безопасности в промышленных и корпоративных системах автоматизации /Лек/	9	4	ПК-1 ПК-3	Л1.1 Л1.2	0	
2.2	Анализ современных киберугроз в промышленных и корпоративных системах автоматизации, актуальные векторы атак на промышленные сети АСУ ТП /Лек/	9	6	ПК-1 ПК-3	Л1.1 Л1.2	0	
2.3	Оценка уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП /Лек/	9	6	ПК-1 ПК-3	Л1.1 Л1.2	0	
2.4	Оценка уязвимостей по отношению к современным киберугрозам промышленных сетей АСУ ТП /Пр/	9	4	ПК-1 ПК-3	Л1.1 Л1.2	0	
2.5	Анализ современных киберугроз в промышленных и корпоративных системах автоматизации, /Пр/	9	4	ПК-1 ПК-3	Л1.1 Л1.2	0	
2.6	Зачет /ИВКР/	9	0,25	ПК-1 ПК-3	Л1.1 Л1.2	0	

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Контрольные вопросы и задания

Тема: 1. Актуальные угрозы и эволюция киберугроз
1. Какие ключевые угрозы информационной безопасности наиболее актуальны для промышленных компаний? Приведите примеры.
2. Как эволюционируют киберугрозы в ответ на внедрение мер защиты (например, фильтрация трафика, сегментация сети)?
3. Какие факторы способствуют увеличению уязвимостей в промышленных сетях (например, цифровизация, IoT)?
4. Какие последствия могут возникнуть при успешной кибератаке на систему управления технологическим процессом (АСУ ТП)?
5. Приведите примеры реальных кибератак на промышленные системы (Stuxnet, Colonial Pipeline, TRITON) и объясните их механизм.
Тема: 2. Типы киберугроз и векторы атак
6. Какие типы киберугроз наиболее распространены в промышленных и корпоративных системах автоматизации (например, ransomware, APT, фишинг)?
7. Какие векторы атак чаще всего используются злоумышленниками для проникновения в промышленные сети АСУ ТП?
8. Почему традиционные средства ИБ (антивирусы, файрволы) недостаточны для защиты АСУ ТП?
9. Как социальная инженерия может стать точкой входа для атаки на промышленную сеть?
10. Какие угрозы возникают из-за взаимодействия корпоративной сети и сети АСУ ТП?
Тема: 3. Средства и меры информационной безопасности
11. Какие специфические меры ИБ применяются в АСУ ТП для защиты от киберугроз (например, DMZ, протокольные брокеры)?
12. Как работают системы обнаружения аномалий (IDS/IPS) в промышленных сетях?
13. Какие стандарты и регуляторы регулируют защиту промышленных систем (например, IEC 62443, NIST SP 800-82)?
14. Как используется микросегментация для минимизации рисков в АСУ ТП?
15. Какие особенности применения шифрования в промышленных протоколах (Modbus, DNP3, IEC 61850)?
Тема: 4. Идентификация и моделирование каналов воздействия
16. Какие методы используются для идентификации каналов возможного деструктивного воздействия в АСУ ТП?
17. Как моделировать сценарии атак на промышленные сети (например, симуляция DDoS, MITM)?
18. Какие уязвимости наиболее критичны для протоколов Modbus и IEC 60870-5-104?
19. Как использовать тестирование на проникновение (пентестинг) для выявления слабых мест в промышленных системах?
20. Какие угрозы возникают из-за устаревших операционных систем (например, Windows XP) в АСУ ТП?
Тема: 5. Анализ и оценка рисков
21. Какие этапы включает процесс оценки рисков ИБ в промышленных системах (идентификация, анализ, лечение)?
22. Какие методологии используются для оценки рисков (например, OCTAVE, FAIR, MEHARI)?
23. Как рассчитывается уровень риска для критически важных технологических процессов?
24. Как влияет взаимодействие с внешними поставщиками на уровень риска?
25. Какие метрики позволяют оценить эффективность реализованных мер ИБ в промышленной среде?
Тема: 6. Современные киберугрозы и векторы атак
26. Какие специфические векторы атак используются для компрометации АСУ ТП (например, эксплуатация уязвимостей в ПЛК, HMI)?
27. Как атаки типа «вредоносное ПО для ОТ» отличаются от традиционных вредоносных программ?
28. Что такое протокольные атаки и как они реализуются в сетях АСУ ТП?

29. Как угрозы со стороны внутренних пользователей (инсайдеры) влияют на безопасность промышленных систем?
30. Как атаки на цепочки поставок (например, поддельные обновления ПО) угрожают промышленным сетям?
Тема: 7. Оценка уязвимостей в АСУ ТП
31. Какие инструменты используются для сканирования уязвимостей в промышленных устройствах (например, Tenable.ot, Claroty)?
32. Какие уязвимости наиболее распространены в системах SCADA и как их классифицируют (CVE, CVSS)?
33. Как оценить критичность уязвимости в АСУ ТП с учетом риска остановки производства?
34. Какие меры предпринимаются для устранения уязвимостей, если обновление ПО невозможно (например, виртуальные патчи)?
35. Как нулевые дни (zero-day) угрожают промышленным системам и как с этим бороться?
Тема: 8. Современные технологии защиты
36. Как работают технологии Zero Trust в промышленных системах?
37. Какие методы детектирования аномалий используются в системах мониторинга безопасности (например, SIEM, XDR)?
38. Как применение блокчейн-технологий может повысить защищенность АСУ ТП?
39. Как искусственный интеллект и машинное обучение используются для обнаружения кибератак в реальном времени?
40. Какие требования предъявляются к логированию событий в АСУ ТП для обеспечения расследования инцидентов?
Тема: 9. Практические аспекты и кейсы
41. Какие шаги необходимо предпринять при обнаружении индикаторов компрометации (IoC) в промышленной сети?
42. Как подготовить план реагирования на инциденты в АСУ ТП?
43. Какие последствия могут быть у атаки на систему электроснабжения (пример: атака на украинскую энергосистему в 2015 г.)?
44. Как обеспечить безопасность удаленного доступа к АСУ ТП (например, через VPN, RDP)?
45. Какие ошибки чаще всего приводят к утечкам данных в промышленных сетях (неправильная конфигурация, слабые пароли)?
Тема: 10. Перспективные направления и стратегии
46. Как интеграция OT и IT влияет на модель угроз и стратегии защиты?
47. Какие меры помогают защитить АСУ ТП от квантовых угроз в будущем?
48. Как использовать цифровые двойники для тестирования устойчивости АСУ ТП к кибератакам?
49. Какие этические и правовые аспекты возникают при тестировании промышленных систем на безопасность?
50. Какие тренды будут определять развитие ИБ в промышленности в ближайшие 5 лет (например, защита IIoT, AI в обнаружении атак)?

5.2. Темы письменных работ

не предусмотрены

5.3. Оценочные средства

Рабочая программа "Современные киберугрозы в промышленных и корпоративных системах автоматизации" 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: зачет в 9 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	Никифоров С. Н.	Методы защиты информации. Защищенные сети	Санкт-Петербург: Лань, 2021
Л1.2	Зенков А. В.	Информационная безопасность и защита информации: учебное пособие для вузов	Москва: Юрайт, 2024

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 "Современные киберугрозы в промышленных и корпоративных системах автоматизации" 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.