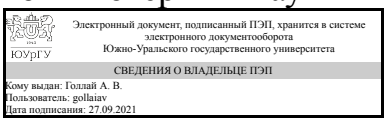
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук



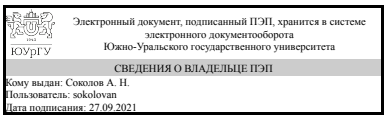
А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины ДВ.1.05.01 Кибербезопасность интеллектуальных автоматизированных систем управления технологическими процессами
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень специалист **тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов
форма обучения очная
кафедра-разработчик Защита информации

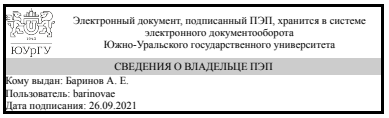
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика,
к.техн.н., доц.



А. Н. Соколов

Разработчик программы,
старший преподаватель



А. Е. Баринов

Челябинск

1. Цели и задачи дисциплины

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. Дисциплина включает материалы, лежащие на стыке двух отраслей: информационная безопасность и автоматизация производств.

Краткое содержание дисциплины

В курсе рассматриваются типовые архитектуры АСУ ТП, угрозы, уязвимости и атаки на АСУ ТП. Основы функциональной безопасности. В качестве прикладных аспектов информационной безопасности основное внимание уделяется защите изолированных сетей, организации DMZ, изучение спецециализированного вредоносного ПО и методов противодействия ему.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-28 способностью управлять информационной безопасностью автоматизированной системы	Знать:Уязвимости современных АСУ ТП. Подходы к устранению уязвимостей в современных промышленных системах Подходы к построению системы защиты современных АСУ ТП Жизненный цикл обеспечения кибербезопасности современных промышленных систем Основы организации своевременной и полноценной обработки инцидентов безопасности Подходы по организации эффективного подразделения центра управления инцидентами (ЦУИ ИБ) для поддержки информационной безопасности промышленной сети
	Уметь:Распознавать атаки социальной инженерии
	Владеть:Навыками исследования пакетов в промышленной сети
ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Знать:Подходы к построению системы защиты современных АСУ ТП
	Уметь:Настраивать межсетевой экран для обеспечения защиты периметра сети Настраивать межсетевой экран для обеспечения сегментации внутренней сети
	Владеть:Навыками разработки политик безопасности современных промышленных систем
ПСК-3.3 способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных	Знать:Структуру АСУ ТП Сетевые технологии, используемые в современных АСУ ТП Отличия обеспечения кибербезопасности современных промышленных систем от обеспечения информационной безопасности в системах общего назначения. Связь обеспечения

объектов	функциональной и информационной безопасности. Проблемы обеспечения кибербезопасности современных промышленных систем Законодательную базу, связанную с обеспечением кибербезопасности современных промышленных систем
	Уметь:Работать со средствами обеспечения безопасности в современных промышленных системах
	Владеть:Навыками анализа инцидентов кибербезопасности в современных промышленных системах

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.30.01 Разработка защищенных автоматизированных систем, Б.1.21 Программно-аппаратные средства обеспечения информационной безопасности, Б.1.22 Организация ЭВМ и вычислительных систем, Б.1.27 Безопасность сетей электронных вычислительных машин	Не предусмотрены

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.22 Организация ЭВМ и вычислительных систем	Знать: архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных и телекоммуникационных систем Уметь: анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем Владеть: методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем
Б.1.30.01 Разработка защищенных автоматизированных систем	Знать: основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Уметь: исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений Владеть: навыками анализа основных узлов и устройств современных автоматизированных систем
Б.1.27 Безопасность сетей электронных вычислительных машин	Знать: принципы построения и функционирования, примеры реализаций

	современных локальных и глобальных компьютерных сетей Уметь: оценивать эффективность и надежность защиты сетей ЭВМ Владеть: навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности
Б.1.21 Программно-аппаратные средства обеспечения информационной безопасности	Знать: программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях Уметь: формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе Владеть: навыками использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 5 з.е., 180 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		9
Общая трудоёмкость дисциплины	180	180
Аудиторные занятия:	80	80
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	16	16
Самостоятельная работа (СРС)	100	100
Безопасность сетей АСУ ТП	23	23
Функциональная безопасность АСУ ТП	8	8
Атаки на интеллектуальные АСУ ТП	8	8
Объект исследования – интеллектуальная АСУ ТП	8	8
Защита изолированных сетей	8	8
Проблема обеспечения кибербезопасности АСУ ТП	8	8
Типовое вредоносное ПО АСУ ТП	14	14
Социальная инженерия	8	8
Организация подразделения обеспечения промышленной кибербезопасности. Политика безопасности	8	8
Введение	7	7
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	экзамен

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах

		Всего	Л	ПЗ	ЛР
1	Введение	2	2	0	0
2	Объект исследования – интеллектуальная АСУ ТП	6	4	2	0
3	Функциональная безопасность АСУ ТП	6	2	4	0
4	Проблема обеспечения кибербезопасности АСУ ТП	10	4	4	2
5	Атаки на интеллектуальные АСУ ТП	12	4	4	4
6	Безопасность сетей АСУ ТП	12	4	4	4
7	Защита изолированных сетей	10	4	4	2
8	Социальная инженерия	6	2	4	0
9	Типовое вредоносное ПО АСУ ТП	10	4	2	4
10	Организация подразделения обеспечения промышленной кибербезопасности. Политика безопасности	6	2	4	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Эволюция АСУ ТП Технологии современных АСУ ТП	2
2	2	Основные определения в области промышленной автоматизации. Модель промышленной системы по ФСТЭК. Модель промышленной системы PERA	2
3	2	Описание современных АСУ ТП как киберфизических систем. Описание современных АСУ ТП как объекта КИИ Типовая архитектура интеллектуальной АСУ ТП	2
4	3	Функциональная безопасность в АСУ ТП. Функциональная и информационная безопасность. Их взаимосвязь и противоречие. Дерево сбоев и атак. Единая модель.	2
5	4	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.	2
6	4	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	2
7	5	Типовая схема вторжения. Атаки на сети промышленных систем. Сканирование сетевых систем. Средства сканирования сетевых систем.	2
8	5	Средства атаки сетевых систем с использованием уязвимостей. Нарушители. Типовые атаки на АСУ ТП. Атаки, связанные с угрозами информационной безопасности. Киберфизические атаки.	2
9	6	Обзор протоколов сетей АСУ ТП. Принципы работы и вопросы безопасности	2
10	6	Обнаружение атак на промышленные сети. Сегментация сетей АСУ ТП. Промышленные межсетевые экраны и IDS.	2
11	7	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	2

		поставщиков и внутренних нарушителей.	
12	7	Угрозы и защита беспроводных коммуникаций в сетях АСУ ТП. Удаленный доступ и его защита.	2
13	8	Фишинг с использованием электронной почты. Признаки фишинга. Направленный фишинг. Фишинг с использованием социальных сетей.	2
14	9	Разбор известных инцидентов атаки промышленных систем посредством вредоносного ПО.	2
15	9	Специализированные средства обнаружения и противодействия вредоносному ПО во внутренней сети промышленных систем.	2
16	10	Подразделение ИБ АСУ ТП. Особенности организации работы. Задачи подразделения кибербезопасности. Взаимодействие с другими структурами	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	2	Анализ структур различных АСУ ТП	2
2	3	Рассмотрение моделей и расчёт рисков функциональной безопасности	4
3	4	Анализ проблем защищённости и выработка требований к защите типовых АСУ ТП	4
4	5	Модель атаки и нарушителя АСУ ТП	4
5	6	Разбор протоколов сетей АСУ ТП	2
6	6	Подходы по интеграции в сеть АСУ ТП защитных решений	2
7	7	Обсуждение проблематики "воздушного зазора"	2
8	7	Атаки на беспроводные сети и способы организации безопасного удалённого доступа	2
9	8	Рассмотрение подходов различных видов социальной инженерии	2
10	8	Программы повышения осведомлённости сотрудников	2
11	9	Обзор типового вредоносного ПО АСУ ТП	2
12	10	Деловая игра по формированию подразделения ИБ АСУ ТП	4

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1	4	Изучение дампов сетевого трафика промышленных протоколов	2
2	5	Обнаружение и исследование уязвимостей промышленных устройств	4
3	6	Сегментация промышленных сетей	2
4	6	Настройка IDS для промышленной сети	2
5	7	Расширенная настройка правил сетевой безопасности для обнаружения целевых атак	2
6	9	Настройка средств обеспечения ИБ уровня конечного узла	2
7	9	Настройка средств централизованного управления средствами обеспечения ИБ в АСУ ТП	2

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием	Кол-во часов

	разделов, глав, страниц)	
Подготовка к лабораторным работам	1. Танненбаум Э. С. Компьютерные сети. 4-е издание, Спб: Издательство "Питер", 2006. ISBN 978-5-318-00492-6 2. Clint Bodungen, Bryan Singer, Aaron Shbeeb, Kyle Wilhoit, Stephen Hilt «Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions», 1st Edition, McGraw-Hill Educationб 2016 3. Gordon Clarke, Deon Reynders «Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems»	34
Подготовка к практическим занятиям	1. Федеральная Служба по Техническому и Экспортному Контролю приказ от 14 марта 2014 г. N 31 «Об утверждении требований к обеспечению за-щиты информации в автоматизированных системах управления производ-ственными и технологическими процессами на критически важных объек-тах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» 2. Ольга Синенко, Надежда Куцевич, Евгений Андреев «SCADA-системы. Взгляд изнутри», РТСофт, 2004	66

6. Инновационные образовательные технологии, используемые в учебном процессе

Не предусмотрены

Собственные инновационные способы и методы, используемые в образовательном процессе

Не предусмотрены

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Введение	ПСК-3.3 способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной	Тестовая проверка знаний	1-15

	безопасности критически важных объектов и автоматизированных систем критически важных объектов		
Объект исследования – интеллектуальная АСУ ТП	ПСК-3.3 способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	Тестовая проверка знаний	16-30
Функциональная безопасность АСУ ТП	ПК-28 способностью управлять информационной безопасностью автоматизированной системы	Тестовая проверка знаний	31-45
Проблема обеспечения кибербезопасности АСУ ТП	ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Приём заданий	46-60
Атаки на интеллектуальные АСУ ТП	ПК-28 способностью управлять информационной безопасностью автоматизированной системы	Приём заданий	61-75
Безопасность сетей АСУ ТП	ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Приём заданий	76-90
Защита изолированных сетей	ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Приём заданий	91-105
Социальная инженерия	ПК-28 способностью управлять информационной безопасностью автоматизированной системы	Тестовая проверка знаний	106-120
Типовое вредоносное ПО АСУ ТП	ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Приём заданий	121-135
Организация подразделения обеспечения промышленной кибербезопасности. Политика безопасности	ПК-28 способностью управлять информационной безопасностью автоматизированной системы	Тестовая проверка знаний	136-150
Все разделы	ПК-28 способностью управлять информационной безопасностью автоматизированной системы	Промежуточный(Экзамен)	1-58

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Тестовая проверка знаний	Тест	Отлично: Правильное выполнение не менее 85% заданий Хорошо: Правильное выполнение не менее 65% заданий

		Удовлетворительно: Правильное выполнение не менее 50% заданий Неудовлетворительно: Правильное выполнение менее 50% заданий
Приём заданий	Защита отчётов лабораторных работ	Отлично: Полное выполнение и полные ответы на доп. вопросы Хорошо: Полное выполнение и ответы на часть доп. вопросов Удовлетворительно: Ошибки в выполнении и неполные ответы на защите Неудовлетворительно: Не выполнение задание или существенные ошибки в ответе на доп. вопросы
Промежуточный(Экзамен)	К экзамену допускаются студенты, выполнившие и защитившие все лабораторные работы. Экзамен проводится в устной форме. Каждому студенту выдается билет, в котором присутствует два теоретических вопроса. При неправильном ответе студенту могут быть заданы уточняющие или новые вопросы по той же теме. Тема считается освоенной, если студент смог ответить на 60% вопроса , заданного по данной теме.	Отлично: Студент должен ответить на более 85% заданных вопросов, наиболее полно раскрыть содержание материала в объеме программы дисциплины, чётко и правильно дать необходимые определения, привести доказательства, показать навыки решения стандартных задач в области защиты баз данных. Ответ должен быть самостоятельный, при ответе использованы приобретённые ранее знания. Хорошо: Студент должен ответить на более 75% заданных вопросов, раскрыть содержание материала в объеме программы дисциплины, в основном правильно дать основные определения и понятия предмета. При ответе могут быть допущены неточности, нарушения последовательности изложения, а также могут быть небольшие неточности при выводах и использовании терминов, практические навыки нетвёрдые. Удовлетворительно: Студент должен ответить на более 60% заданных вопросов, усвоить основное содержание материала в объеме программы дисциплины. При ответе определения и понятия даны не чётко, допущены ошибки в выводах, практические навыки слабые. Неудовлетворительно: Студент ответил менее чем на 59% заданных вопросов, не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач, основное содержание учебного материала не раскрыто. При ответе допущены грубые ошибки в

		определениях, не даны ответы на дополнительные вопросы преподавателя, отсутствуют навыки решения стандартных задач в области защиты баз данных.

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Тестовая проверка знаний	Тестирование по курсу осуществляется на платформе https://certification.kaspersky.com согласно лицензионному соглашению на материалы курса с АО "Лаборатория Касперского"
Приём заданий	Отчет каждой лабораторной работы должен содержать следующие материалы: Краткие теоретические сведения Основные этапы работы Выводы Ответы на контрольные вопросы Основы кибербезопасности интеллектуальных энергосистем. Лабораторный практикум.pdf
Промежуточный(Экзамен)	1.1. Эволюция АСУ ТП 1.2. Технологии современных АСУ ТП 2.1. Основные определения в области промышленной автоматизации. 2.2. Модель промышленной системы по ФСТЭК. 2.3. Модель промышленной системы PERA 2.4. Описание современных АСУ ТП как киберфизических систем. 2.5. Описание современных АСУ ТП как объекта КИИ 2.6. Типовая архитектура интеллектуальной АСУ ТП 3.1. Функциональная безопасность в АСУ ТП. 3.2. Функциональная и информационная безопасность. Их взаимосвязь и противоречие. 3.3. Дерево сбоев и атак. Единая модель. 4.1. Нормативные документы Российской федерации в области кибербезопасности. 31 приказ ФСТЭК и другие документы 4.2. Федеральный закон 187 4.3. Международные нормативные документы. Документы NERC CIP, NIST 4.4. Понятие эшелонированной защиты. 4.5. Трудности при внедрении эшелонированной защиты. 4.6. Проблемы обеспечения безопасности современных промышленных систем. Атаки на современные промышленные системы – общие положения. 4.7. Уязвимости современных промышленных системы – причины. 4.8. Устранение уязвимостей. Обновление программного обеспечения промышленных систем. Проблемы устранения уязвимостей и способы их решения. 4.9. Отличительные особенности и проблемы обеспечения методов обеспечения кибербезопасности промышленных предприятий. 4.10. Угрозы информационной безопасности в АСУ ТП. Объекты защиты АСУ ТП 5.1. Типовая схема вторжения. 5.2. Атаки на сети промышленных систем. Сканирование сетевых систем. Средства сканирования сетевых систем. 5.3. Средства атаки сетевых систем с использованием уязвимостей. 5.4. Нарушители. Типовые атаки на АСУ ТП. Атаки, связанные с

	угрозами информационной безопасности. Киберфизические атаки. 6.1. Обзор протоколов сетей АСУ ТП. Принципы работы и вопросы безопасности 6.2. Обнаружение атак на промышленные сети. Сегментация сетей АСУ ТП. Промышленные межсетевые экраны и IDS. 7.1. Понятие «воздушного зазора». Способы атак на промышленные системы, не подключенные к сети Интернет. 7.2. Преодоление «воздушного зазора». Сменные носители. Политика использования сменных носителей 7.3. Атака со стороны поставщиков и внутренних нарушителей. Методы защиты от атак со стороны поставщиков и внутренних нарушителей. 7.4. Угрозы и защита беспроводных коммуникаций в сетях АСУ ТП. 7.5. Удаленный доступ и его защита. 8.1. Фишинг с использованием электронной почты. Признаки фишинга. Направленный фишинг. 8.2. Фишинг с использованием социальных сетей. 9.1. Разбор известных инцидентов атаки промышленных систем посредством вредоносного ПО. 9.2. Специализированные средства обнаружения и противодействия вредоносному ПО во внутренней сети промышленных систем. 10. Подразделение ИБ АСУ ТП. Особенности организации работы. Задачи подразделения кибербезопасности. Взаимодействие с другими структурами

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

г) методические указания для студентов по освоению дисциплины:

1. Баринов А.Е. Методические указания по дисциплине "Кибербезопасность интеллектуальных автоматизированных систем управления технологическими процессами"

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Основная литература	Сергеев, А. Н. Основы локальных компьютерных сетей : учебное пособие для	Электронно-библиотечная	Интернет / Авторизованный

		вузов / А. Н. Сергеев. — 3-е изд., стер. — Санкт-Петербург : Лань, 2021. — 184 с. — ISBN 978-5-8114-6855-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152651 (дата обращения: 16.09.2021). — Режим доступа: для авториз. пользователей.	система издательства Лань	
2	Дополнительная литература	Интегрированные системы проектирования и управления. SCADA : учебное пособие / Х. Н. Музипов, О. Н. Кузяков, С. А. Хохрин [и др.]. — Санкт-Петербург : Лань, 2021. — 408 с. — ISBN 978-5-8114-3265-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/169310 (дата обращения: 16.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
3	Дополнительная литература	Дадаян, Л. Г. Автоматизированные системы управления технологическими процессами : учебное пособие / Л. Г. Дадаян. — Уфа : УГНТУ, 2018. — 241 с. — ISBN 978-5-7831-1676-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/166886 (дата обращения: 16.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

Нет

Перечень используемых информационных справочных систем:

Нет

10. Материально-техническое обеспечение дисциплины

Не предусмотрено