ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ»

УТВЕРЖДАЮ

Ректор

_____ / Ю.Ю. Михальчевский

«17» июня 2021 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность

Направление подготовки
25.04.04 Эксплуатация аэропортов и обеспечение полетов воздушных судов

Направленность программы (профиль)
Управление аэропортовой деятельностью

Квалификация выпускника
магистр

Форма обучения
заочная

Санкт-Петербург
2021

1 Цели освоения дисциплины

Целью освоения дисциплины «Информационная безопасность» является формирование у студентов системы знаний и умений в области информационной безопасности компьютерных систем и применения на практике средств защиты информации.

Задачами освоения дисциплины являются:

- изучение современного состояния обеспечения различных направлений информационной безопасности;
- освоение базовой терминологии, использующейся в сфере обеспечения информационной безопасности;
- освоение нормативно-правовой базы по обеспечению информационной безопасности;
- формирование знаний о структуре и основных требованиях стандартов, в сфере информационной безопасности;
- формирование представлений о механизмах формирования политики информационной безопасности.

Дисциплина обеспечивает подготовку обучающегося к решению задач профессиональной деятельности организационно-управленческого и научно-исследовательского типов.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность» представляет собой дисциплину, относящуюся к обязательной части Блока 1 Дисциплины (модули).

Дисциплина «Информационная безопасность» базируется на результатах обучения, полученных при изучении дисциплин: «Инновационный менеджмент»; «Управление транспортной безопасностью»; «Управление человеческими ресурсами».

Дисциплина «Информационная безопасность» является обеспечивающей для дисциплин, практик: «Управление проектами»; «Управление коммерческой деятельностью оператора аэропорта (аэродрома)»; «Стратегическое планирование и управление аэропортом»; «Автоматизация производственной и коммерческой деятельности оператора аэропорта (аэродрома)»; «Производственно-технологическая практика»; «Научно-исследовательская работа».

Дисциплина изучается во 2 семестре.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс освоения дисциплины «Информационная безопасность» направлен на формирование следующих компетенций:

Код компетенции/ индикатора	Результат обучения: наименование компетенции, индикатора компетенции
ОПК-10	Способен к выявлению и анализу опасностей и угроз, возникающих в процессе развития современного информационного общества
ОПК-10.1	Прогнозирует эффективность функционирования систем обеспечения безопасности, оценивая затраты и риски
ОПК-10.2	Анализирует угрозы обеспечения безопасности объектов и разрабатывает методы противодействия им
ОПК-10.3	Осуществляет построение как отдельных процессов управления информационной безопасностью, так и системы процессов в целом
ОПК-11	Способен организовывать и обеспечивать соблюдение основных требований информационной безопасности, в том числе защиту охраняемой законом тайны
ОПК-11.1	Анализирует направления развития информационно-коммуникационных технологий объекта защиты
ОПК-11.2	Анализирует текущее состояние информационной безопасности на предприятии с целью разработки требований к разрабатываемым процессам управления информационной безопасностью
ОПК-11.3	Применяет процессный подход к управлению информационной безопасностью в сферах деятельности области аэронавигации

Планируемые результаты изучения дисциплины:

Знать:

- основные пути и методы решения задач в области создания режима информационной безопасности систем автоматизации воздушного транспорта;
- требования нормативно-правовой базы в области обеспечения информационной безопасности на предприятиях гражданской авиации;
- основные возможности и характеристики программных и аппаратных средств обеспечения защиты информации.

Уметь:

- определять «узкие» места в системе обеспечения информационной безопасности, и предлагать пути их устранения;
- грамотно эксплуатировать программные средства информационной безопасности.

Владеть:

- методикой разработки и внедрения систем информационной безопасности в структурных подразделениях системы воздушного транспорта**;**

- программными средствами защиты информации при работе с компьютерными системами, включая приёмы антивирусной защиты.

4 Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины (модуля) составляет 2 зачетных единицы 72 академических часа.

Наименование	Всего часов	Семестр
		2
Общая трудоемкость дисциплины	72	72
Контактная работа, всего	8,3	8,3
лекции	4	4
практические занятия	4	4
лабораторные работы	-	-
курсовой проект (работа)	-	-
Самостоятельная работа студента	55	55
Промежуточная аттестация	9	9
контактная работа	0,3	0,3
самостоятельная работа по подготовке к зачету	8,7 Зачет	8,7 Зачет

5 Содержание дисциплины

5.1 Соотнесения тем (разделов) дисциплины и формируемых компетенций

Темы дисциплины	Количество часов	Компетенции		Образовательные технологии	Оценочные средства
		ОПК-10	ОПК-11		
Тема 1. Задачи по обеспечению информационной безопасности компьютерных систем	5,5	+	+	ВК, Л, СРС	У
Тема 2. Уровни обеспечения информационной безопасности	6,5	+	+	ПЗ, СРС	У
Тема 3. Анализ угроз информационной безопасности.	9	+	+	Л, ПЗ, СРС	У

Темы дисциплины	Количество часов	Компетенции		Образовательные технологии	Оценочные средства
		ОПК-10	ОПК-11		
Тема .4. Таксономия критериев информационной безопасности.	9	+	+	ИЛ, ИПЗ, СРС	У
Тема 5. Защита информационных систем от вредоносного программного обеспечения	9,5	+	+	ИЛ, ПЗ, ИПЗ, СРС	У
Тема 6. Межсетевое экранирование	10	+	+	ИЛ, ПЗ, ИПЗ, СРС	У
Тема 7. Защита персональных данных	7,2	+	+	Л, ПЗ, СРС	У
Тема 8. Безопасность критической информационной инфраструктуры	6,3	+	+	ПЗ, СРС	У
Итого по дисциплине	63				
Промежуточная аттестация	9				Зачет
Всего по дисциплине	72				

Сокращения: Л − лекция, ИЛ - интерактивная лекция, ПЗ- практические занятия, ИПЗ – интерактивное практическое занятие, СРС − самостоятельная работа студента, ВК − входной контроль, У − устный опрос.

5.2 Темы (разделы) дисциплины и виды занятий

Наименование темы дисциплины	Л	ПЗ	ЛР	СРС	КП	Всего часов
Тема 1. Задачи по обеспечению информационной безопасности компьютерных систем	0,5	-	-	5	-	5,5
Тема 2. Уровни обеспечения Информационной безопасности	-	0,5	-	6	-	6,5
Тема 3. Анализ угроз информационной безопасности.	0,5	0,5	-	8	-	9
Тема .4. Таксономия критериев информационной безопасности.	0,5	0,5	-	8	-	9
Тема 5. Защита информационных систем от вредоносного программного обеспечения	0,5	1	-	8	-	9,5
Тема 6. Межсетевое экранирование	1	1	-	8	-	10
Тема 7 Защита персональных данных	1	0,2	-	6	-	7,2
Тема. 8 Безопасность критической информационной инфраструктуры	-	0,3	-	6	-	6,3
Итого по дисциплине	4	4	-	55	-	63
Промежуточная аттестация						9
Всего по дисциплине						72

Сокращения: Л – лекция, ПЗ – практическое занятие, ЛР – лабораторная работа, СРС – самостоятельная работа студента, КП – курсовой проект.

5.3 Содержание дисциплины

Тема 1. Задачи по обеспечению информационной безопасности компьютерных систем

Значение информационной безопасности компьютерных систем для стабильного функционирования предприятий и организаций системы воздушного транспорта. Определение понятия «информационная безопасность», практические аспекты информационной безопасности.

Тема 2. Тема 2. Уровни обеспечения Информационной безопасности

Законодательный, административный, процедурный и программно-технический уровни обеспечения информационной безопасности. Политика информационной безопасности предприятия.

Тема 3. Анализ угроз информационной безопасности

Классификация и анализ угроз информационной безопасности компьютерных систем. Оценка угроз информационной безопасности.

Тема 4. Таксономия критериев информационной безопасности

Стандарты по информационной безопасности. «Оранжевая книга», её значение и содержание. Механизмы создания и поддержания надежной вычислительной базы.

Тема 5. Защита информационных систем от вредоносного программного обеспечения

Классификация вредоносного программного обеспечения. Компьютерные вирусы, троянские программы, сетевые компьютерные черви, и другое вредоносное программное обеспечение. Классификация средств борьбы с вредоносным программным обеспечением.

Тема 6. Межсетевое экранирование

Эталонная модель взаимодействия открытых систем: её назначение и функционирование. Комплексный межсетевой экран, состав, назначение составляющих элементов.

Тема 7. Защита персональный данных

Обзор законодательной базы защиты персональных данных. Анализ угроз персональным данным. Формирование требований к информационным системам, обрабатывающим персональные данные. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных и автоматизированных системах, а также, при передаче по телекоммуникационным каналам связи.

Теме 8. Безопасность критической информационной инфраструктуры

Обзор законодательной базы по обеспечению безопасности объектов критический информационной инфраструктуры. Категорирование объектов КИИ, требования к системам безопасности по обеспечению безопасности значимых объектов КИИ. Практические рекомендации по обеспечению защиты объектов критической информационной инфраструктуры.

5.4 Практические занятия (семинары)

Номер темы дисциплины	Тематика практических занятий	Трудо-емкость (часы)
2	Практическое занятие 1. Уровни обеспечения информационной безопасности. Входной контроль.	0,5

Номер темы дисциплины	Тематика практических занятий	Трудо-емкость (часы)
	Устный опрос.	
3	Практическое занятие 2. Угрозы информационной безопасности. Устный опрос.	0,5
4	Практическое занятие 3. Таксономия критериев информационной безопасности. Устный опрос.	0,5
5	Практическое занятие 4. Противодействие несанкционированному межсетевому доступу. Устный опрос.	0,5
5	Практическое занятие 5. Компьютерные вирусы, троянские программы, сетевые компьютерные черви. Устный опрос.	0,5
6	Практическое занятие 6. Вредоносное программное обеспечение. Устный опрос.	0,5
6	Практическое занятие 7. Средства борьбы с вредоносным программным обеспечением. Устный опрос.	0,5
7	Практическое занятие 8. Защита персональных данных. Устный опрос.	0,2
8	Практическое занятие 9. Безопасность критической информационной инфраструктуры. Устный опрос.	0,3
Итого по дисциплине		**4**

5.5 Лабораторный практикум

Лабораторный практикум учебным планом не предусмотрен.

5.6. Самостоятельная работа

Номер темы дисциплины	Виды самостоятельной работы	Трудоемкость (часы)
1	Самостоятельное овладение студентами материала темы. [4] Подготовка к устному опросу.	5
2	Самостоятельное овладение студентами материала темы [2, 5] Выполнение задания в соответствии с инструкциями и методическими указаниями преподавателя. Подготовка к устному опросу.	6
3	Самостоятельное овладение студентами материала темы [1,2,3,6] Выполнение задания в соответствии с инструкциями и методическими указаниями преподавателя. Подготовка к устному опросу.	8
4	Самостоятельное овладение студентами материала темы [3] Выполнение задания в соответствии с инструкциями и методическими указаниями преподавателя. Подготовка к устному опросу.	8
5	Самостоятельное овладение студентами материала темы [2,4] Выполнение задания в соответствии с инструкциями и методическими указаниями преподавателя. Подготовка к устному опросу.	8
6	Самостоятельное овладение студентами материала темы [1,3] Выполнение задания в соответствии с инструкциями и методическими указаниями преподавателя. Подготовка к устному опросу.	8
7	Самостоятельное овладение студентами материала темы [1,3] Выполнение задания в соответствии с инструкциями и методическими указаниями преподавателя. Подготовка к устному опросу.	6

Номер темы дисциплины	Виды самостоятельной работы	Трудоемкость (часы)
8	Самостоятельное овладение студентами материала темы [1,3] Выполнение задания в соответствии с инструкциями и методическими указаниями преподавателя. Подготовка к устному опросу.	6
Итого по дисциплине		55

5.7 Курсовые работы

Курсовые работы (проекты) учебным планом не предусмотрены.

6 Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Шаньгин В.Ф. Информационная безопасность и защита информации [Текст] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2014. - 702с. - ISBN 978-5-97060-226-3.

2. Баранова Е.К. Информационная безопасность и защита информации :Учеб. пособ. для вузов [Текст] / Е. К. Баранова, А. В. Бабаш, А. М. Петраков. - 2-е изд. - М.: РИОР-Инфра-М, 2014. - 256с.

б) дополнительная литература:

3. Нестеров С.А. Информационная безопасность: Учебник и практикум для академического бакалавриата. Реком. УМО [Текст] / С. А. Нестеров. - М.: Юрайт, 2016. - 321с. - ISBN 978-5-9916-7227-6.

4. Мельников В.П. Информационная безопасность и защита информации: Учеб. пособ. для вузов. Допущ. УМО [Текст] / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - 2-е изд. стереотип. - М.: Академия, 2007. - 336с.

5. Бирюков А.А. Информационная безопасность: защита и нападение. [Текст] / А. А. Бирюков. - М.: ДМК Пресс, 2016. - 474с. - ISBN 978-5-97060-226-3.

6. Ярочкин В.И. Информационная безопасность: Учеб. для вузов. Реком. Минобр. РФ [Текст] / В. И. Ярочкин. - М.: Академ. проспект, 2006. - 544с.

в) перечень ресурсов информационно-телекоммуникационной сети «Интернет»:

7. https://www.intuit.ru/studies/courses/10/10/lecture/296?page=1
8. https://www.intuit.ru/studies/courses/10/10/lecture/302
9. https://www.intuit.ru/studies/courses/3649/891/lecture/32336?page=1
10. https://www.intuit.ru/studies/courses/10/10/lecture/306
11. https://www.intuit.ru/studies/courses/10/10/lecture/310
12. https://www.intuit.ru/studies/courses/10/10/lecture/312

13. https://www.intuit.ru/studies/courses/10/10/lecture/300
14. https://studref.com/325272/informatika/klassifikatsiya_ugroz_informatsionnoy_bezopasnosti#846
15. http://protect.htmlweb.ru/orange1.htm
16. https://studfiles.net/preview/3103252/page:8/
17. https://www.kazedu.kz/referat/84974/4
18. https://www.kazedu.kz/referat/84974/5
19. https://www.kazedu.kz/referat/84974/8
20. https://ocompah.ru/razlichie-mezhdu-kompyuternyj-virus-cherv-troyanskij-kon.html
21. http://old.intuit.ru/department/security/antiviruskasp/2/
22. http://old.intuit.ru/department/security/antiviruskasp/2/2.html#sect3
23. http://old.intuit.ru/department/security/antiviruskasp/5/
24. http://old.intuit.ru/department/security/antiviruskasp/6/
25. http://old.intuit.ru/department/security/antiviruskasp/7/
26. https://www.itweek.ru/security/article/detail.php?ID=104405
27. https://studfiles.net/preview/5282711/
28. http://routeworld.ru/80-model-vzaimodeystviya-otkrytyh-sistem-osi.html
29. http://citforum.ru/nets/protocols/1_01_02.shtml
30. https://studfiles.net/preview/5970826/page:56/
31. https://studfiles.net/preview/5970826/page:57/
32. https://studfiles.net/preview/5970826/page:58/
33. https://studfiles.net/preview/5970826/page:59/
34. http://ypn.ru/322/osi-depended-firewall-functioning-features/
35. https://vuzlit.ru/986869/protivodeystvie_nesanktsionirovannomu_mezhsetevomu_dostupu

г) программное обеспечение (лицензионное), базы данных, информационно-справочные и поисковые системы:

36. Консультант Плюс. Официальный сайт компании [Электронный ресурс]. – Режим доступа: http://www.consultant.ru, свободный (дата обращения 12.01.2021 г.).

37. Гарант. Официальный сайт компании [Электронный ресурс]. – Режим доступа: http://www.garant.ru/products/bank, свободный (дата обращения 12.01.2021 г.).

38. Издательство «ЮРайт». Официальный сайт издательства [Электронный ресурс]. – Режим доступа: http://urait.ru.

39. Открытая база ГОСТов. [Электронный ресурс]. – Режим доступа: http://standartgost.ru, свободный (дата обращения 12.01.2021 г.).

40. Электронная библиотека научных публикаций «eLIBRARY.RU» [Электронный ресурс]. − Режим доступа: http://elibrary.ru, свободный (дата обращения 12.01.2021 г.).

41. Электронно-библиотечная система издательства «Лань» [Электронный ресурс]. − Режим доступа: URL: http://e.lanbook.com.

42. Сканер уязвимостей XSpider фирмы Positive Technologies;

43. Комплексная система контроля защищённости MaxPatrol 8 фирмы Positive Technologies;

44. Антивирусный пакет Kaspersky Endpoint Security Standard for Windows.

7 Материально-техническое обеспечение дисциплины

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Аудитория № 400 Компьютерный класс	Комплект учебной мебели – 24 шт. Проектор Panasonic PT – ST 10 – 1 шт. Экран – 1 шт. Доска меловая – 1 шт. Компьютеры – 24 шт.

8 Образовательные и информационные технологии

Входной контроль проводится в форме устных опросов с целью оценивания остаточных знаний по ранее изученным дисциплинам или разделам изучаемой дисциплины.

При изучении дисциплины используются как традиционные **лекции**, так и интерактивные лекции.

Интерактивные лекции проводятся в нескольких вариантах

-п**роблемная лекция** начинается с постановки проблемы, которую необходимо решить в процессе изложения материала.

-лекция-визуализация учит студентов преобразовывать устную и письменную информацию в визуальную форму, что формирует у них профессиональное мышление за счет систематизации и выделения наиболее значимых, существенных элементов содержания обучения.

- лекция-беседа предполагает непосредственный контакт преподавателя с аудиторией, позволяет привлечь внимание студентов к наиболее важным вопросам темы, вовлечь в двусторонний обмен мнениями, выяснить уровень их осведомленности по рассматриваемой теме, степени их готовности к восприятию последующего материала, позволяет адресовать вопрос к конкретному студенту, спросить его мнение по обсуждаемой проблеме.

-лекция-дискуссия - преподаватель при изложении лекционного материала не только использует ответы студентов на свои вопросы, но и организует свободный обмен мнениями в интервалах между логическими разделами.

Практические занятия проводятся с использованием специальных компьютерных программ и предназначены для закрепления полученных знаний, а также выработки необходимых умений и навыков.

Интерактивное практическое занятие проводится с использование средств вычислительной техники и специального программного обеспечения, и предполагает выполнение выданных конкретных заданий.

Самостоятельная работа студента проводится с целью закрепления и совершенствования осваиваемых компетенций, предполагает сочетание самостоятельных теоретических занятий и самостоятельное выполнение практических заданий, описанных в рекомендованной литературе [1,2].

Зачет - промежуточная аттестация, оценивающая уровень освоения компетенций по итогам освоения дисциплины.

Зачет – устные ответы на 2 теоретических вопроса из перечня вопросов на зачет и решение задачи.

Описание шкалы оценивания, используемой для проведения промежуточных аттестаций приведено в п.9.5.

К моменту сдачи зачета должны быть успешно пройдены предыдущие формы контроля.

9 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины

Фонд оценочных средств по дисциплине предназначен для выявления и оценки уровня и качества знаний студентов по результатам текущего контроля и промежуточной аттестации по итогам освоения дисциплины в форме зачета.

Фонд оценочных средств для текущего контроля включает вопросы для устного опроса.

Устный опрос, как правило, в течение 10 минут по темам в соответствии с данной программой и предназначено для проверки обучающихся на предмет освоения пройденного материала.

Промежуточная аттестация по итогам освоения дисциплины проводится во втором семестре в форме зачета. Этот вид промежуточной аттестации позволяет оценить уровень освоения студентом компетенций за весь период изучения дисциплины. Зачет предполагает устный ответ на 2 теоретических вопроса.

Методика формирования результирующей оценки в обязательном порядке учитывает активность студентов на лекциях и практических занятиях, участие студентов в конференциях и подготовку ими публикаций. Описание шкалы оценивания, используемой для проведения промежуточной аттестации, приведено в п. 9.5.

9.1 Балльно-рейтинговая оценка текущего контроля успеваемости и знаний студентов

Балльно-рейтинговая оценка текущего контроля успеваемости и знаний студентов не применяется.

9.2 Методические рекомендации по проведению процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура оценивания знаний, умений и навыков, характеризующих этапы формирования компетенций, предусматривает текущий контроль успеваемости обучающихся и промежуточную аттестацию по итогам освоения дисциплины. При этом фонд оценочных средств включает следующие оценочные средства и шкалы оценивания.

Оценочные средства	Шкалы оценивания*
Текущий контроль успеваемости обучающихся	
Тест	«Отлично»: правильные ответы даны на не менее чем 85 % вопросов. «Хорошо»: правильные ответы даны на не менее чем 75 % вопросов. «Удовлетворительно»: правильные ответы даны на не менее чем 60 % вопросов. «Неудовлетворительно»: правильные ответы даны на 59% и менее вопросов.
Устный опрос	«Отлично»: обучающийся четко и ясно, по существу дает ответ на поставленный вопрос. «Хорошо»: обучающийся дает ответ на поставленный вопрос по существу и правильно отвечает на уточняющие вопросы. «Удовлетворительно»: обучающийся не сразу дал верный ответ, но смог дать его правильно при помощи ответов на наводящие вопросы. «Неудовлетворительно»: обучающийся отказывается отвечать на поставленный вопрос, либо отвечает на него неверно и при формулировании дополнительных (вспомогательных) вопросов.
Доклад	«Отлично»: обучающийся делает доклад, полностью соответствующий требованиям. «Хорошо»: обучающийся делает доклад, частично соответствующий требованиям. «Удовлетворительно»: обучающийся делает доклад, частично соответствующий требованиям с незначительными ошибками. «Неудовлетворительно»: обучающийся делает доклад либо частично соответствующий требованиям со значительными ошибками, либо полностью несоответствующий требованиям. Требования к докладу определяются индивидуально исходя из темы исследования.
Учебное задание	«Отлично»: задание выполнено полностью, в соответствии с поставленными требованиями; при ответе обучающийся демонстрирует знание программного материала; ответ обучающегося аргументирован и не содержит ошибок. «Хорошо»: задание выполнено полностью, в соответствии с поставленными требованиями; при ответе обучающийся демонстрирует знание программного материала; ответ обучающегося аргументирован, но дан с незначительными ошибками. «Удовлетворительно»: задание выполнено полностью, в соответствии с поставленными требованиями; при ответе обучающийся в недостаточной степени демонстрирует знание программного материала; ответ обучающегося в недостаточной степени аргументирован и дан с незначительными ошибками. «Неудовлетворительно»: обучающийся не выполнил задания, или результат выполнения задания не соответствует поставленным требованиям; обучающийся демонстрирует незнание программного материала; обучающийся не может аргументировать свой ответ; в заданиях и (или) ответах имеются существенные ошибки.

9.3. Темы курсовых работ (проектов) по дисциплине

В учебном плане написание курсовых работ не предусмотрено.

9.4 Контрольные вопросы для проведения входного контроля остаточных знаний по обеспечивающим дисциплинам

1. Общее понятие безопасности.
2. Основные причины, вызывающие возрастание значения безопасности РФ в современных условиях.
3. Основные документы, определяющие понятия «безопасность РФ» и «национальная безопасность РФ».
4. Основные термины и определения, связанные с понятием безопасности на транспорте.
5. Понятие комплексной системы обеспечения безопасности.
6. Основные направления нормативно-правовой деятельности в области обеспечения безопасности на транспорте и их характеристика.
7. Основные направления организационной деятельности по обеспечению безопасности на транспорте и их характеристика.

9.5 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Показатели и критерии оценивания компетенций на различных этапах их формирования

Компетенции	Показатели оценивания (индикаторы достижения) компетенций	Критерии оценивания
I этап		
ОПК-10; ОПК-11	ОПК-10.1; ОПК-10.2; ОПК-10.3; ОПК-11.1; ОПК-11.2; ОПК-11.3	Знает: - основные пути и методы решения задач в области создания режима информационной безопасности систем автоматизации воздушного транспорта; - требования нормативно-правовой базы в области обеспечения информационной безопасности на предприятиях гражданской авиации; - основные возможности и характеристики программных и аппаратных средств обеспечения защиты

Компетенции	Показатели оценивания (индикаторы достижения) компетенций	Критерии оценивания
		информации.
II этап		
ОПК-10; ОПК-11	ОПК-10.1; ОПК-10.2; ОПК-10.3; ОПК-11.1; ОПК-11.2; ОПК-11.3	Умеет: - определять «узкие» места в системе обеспечения информационной безопасности, и предлагать пути их устранения; - грамотно эксплуатировать программные средства информационной безопасности. Владеет: - методикой разработки и внедрения систем информационной безопасности в структурных подразделениях системы воздушного транспорта**;** - программными средствами защиты информации при работе с компьютерными системами, включая приёмы антивирусной защиты.

Шкала оценивания при проведении промежуточной аттестации

Зачет

На зачет выносятся вопросы, охватывающие все содержание учебной дисциплины.

Знания обучающихся оцениваются по системе с выставлением, обучающимся итоговой оценки «зачтено», либо «не зачтено»

«Зачтено» при приеме зачета выставляется в случае:

− полного, правильного и уверенного изложения обучающимся учебного материала по каждому из вопросов билета;

− уверенного владения обучающимся понятийно-категориальным аппаратом учебной дисциплины;

− логически последовательного, взаимосвязанного и правильно структурированного изложения обучающимся учебного материала, умения устанавливать и прослеживать причинно-следственные связи между событиями, процессами и явлениями, о которых идет речь в вопросах билета;

− приведения обучающимся надлежащей аргументации, наличия у обучающегося логически и нормативно обоснованной точки зрения при освещении проблемных, дискуссионных аспектов учебного материала по вопросам билета;

− лаконичного и правильного ответа обучающегося на дополнительные вопросы преподавателя.

«Не зачтено» при приеме зачета выставляется в случае:

− невозможности изложения обучающимся учебного материала по любому из вопросов билета при условии полного, правильного и уверенного изложения учебного материала по как минимум одному из вопросов билета;

− допущения обучающимся существенных ошибок при изложении учебного материала по отдельным (одному или двум) вопросам билета;

− допущении обучающимся ошибок при использовании в ходе ответа основных понятий и категорий учебной дисциплины;

− существенного нарушения обучающимся или отсутствия у обучающегося логической последовательности, взаимосвязи и структуры изложения учебного материала, неумения обучающегося устанавливать и прослеживать причинно-следственные связи между событиями, процессами и явлениями, о которых идет речь в вопросах билета;

− отсутствия у обучающегося аргументации, логически и нормативно обоснованной точки зрения при освещении проблемных, дискуссионных аспектов учебного материала по вопросам билета;

− невозможности обучающегося дать ответы на дополнительные вопросы преподавателя.

Дополнительные вопросы могут быть заданы обучающемуся в случае:

− необходимости конкретизации и изложенной обучающимся информации по вопросам билета с целью проверки глубины знаний отвечающего по связанным между собой темам и проблемам;

− необходимости проверки знаний обучающегося по основным темам и проблемам курса при недостаточной полноте его ответа по вопросам билета.

9.6 Типовые контрольные задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины

Примерный перечень вопросов для устного опроса:

1. Дать определение понятию «Информационная безопасность»;
2. Объяснить понятие практического аспекта информационной безопасности «Доступность»;
3. Объяснить понятие практического аспекта информационной безопасности «Целостность»;
4. Объяснить понятие практического аспекта информационной безопасности «Конфиденциальность»;
5. Законодательный уровень обеспечения информационной безопасности. Что это такое? Что входит в это понятие? Примеры законодательных актов;
6. Административный уровень обеспечения информационной безопасности. Понятие «Политика безопасности». Уровни детализации административного уровня, их содержание;

7. Программа безопасности. Её синхронизация с жизненным циклом информационных систем;

8. Процедурный уровень обеспечения информационной безопасности. Что это такое? Классы мер процедурного уровня;

9. Процедурный уровень обеспечения информационной безопасности. Управление персоналом;

10. Процедурный уровень обеспечения информационной безопасности. Физическая защита.

11. Процедурный уровень обеспечения информационной безопасности. Поддержание работоспособности;

12. Процедурный уровень обеспечения информационной безопасности. Реагирование на нарушения режима безопасности;

13. Процедурный уровень обеспечения информационной безопасности. Планирование восстановительных работ;

13. Программно-технический уровень обеспечения информационной безопасности. Сервисы программно-технического уровня:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- шифрование;
- контроль целостности;
- экранирование;
- анализ защищённости;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелирование;
- управление.

14. «Критерии безопасности компьютерных систем» (Оранжевая книга). Таксономия требований. Общие понятия.

15. «Критерии безопасности компьютерных систем» (Оранжевая книга). Таксономия требований. Понятие «Политика безопасности»и её механизмы;

16. «Критерии безопасности компьютерных систем» (Оранжевая книга). Таксономия требований. Понятие «Аудит» и его механизмы;

17. «Критерии безопасности компьютерных систем» (Оранжевая книга). Таксономия требований. Понятие «Корректность» (Гарантированности) и её механизмы;

18. «Критерии безопасности компьютерных систем» (Оранжевая книга). Таксономия требований. Понятие «Документация» и её содержание;

19. Классификация угроз информационной безопасности;

20. Эталонная модель взаимодействия открытых систем. Назначение.

21. Эталонная модель взаимодействия открытых систем. Структура.

22. Эталонная модель взаимодействия открытых систем. Функции уровней.

23. Эталонная модель взаимодействия открытых систем. Прохождение пакетов через ЭМВОС при передаче данных.

24. Комплексный межсетевой экран. Назначение.

25. Комплексный межсетевой экран. Состав.

26. Комплексный межсетевой экран. Экранирующий маршрутизатор. Его назначение.

27. Комплексный межсетевой экран. Экранирующий маршрутизатор. Выполняемые защитные функции.

28. Комплексный межсетевой экран. Экранирующий маршрутизатор. Достоинства и недостатки.

29. Комплексный межсетевой экран. Шлюз сеансового уровня. Назначение.

30. Комплексный межсетевой экран. Шлюз сеансового уровня. Выполняемые защитные функции.

31. Комплексный межсетевой экран. Шлюз сеансового уровня. Функция обеспечения виртуального соединения.

32. Комплексный межсетевой экран. Шлюз сеансового уровня. Процедура квитирования связи по протоколу TCP/IP.

33. Комплексный межсетевой экран. Шлюз сеансового уровня. Трансляция внутренних IP-адресов.

34. Комплексный межсетевой экран. Шлюз сеансового уровня. Достоинства и недостатки.

35. Комплексный межсетевой экран. Шлюз прикладного уровня. Назначение.

36. Комплексный межсетевой экран. Шлюз прикладного уровня. Выполняемые защитные функции.

37. Комплексный межсетевой экран. Шлюз прикладного уровня. Программные посредники.

38. Комплексный межсетевой экран. Шлюз прикладного уровня. Достоинства и недостатки.

39. Вредоносное программное обеспечение. Классификация (виды).

40. Вредоносное программное обеспечение. Компьютерные вирусы. Классификация.

41. Вредоносное программное обеспечение. Компьютерные вирусы. Файловый нерезедентный вирус.

42. Вредоносное программное обеспечение. Компьютерные вирусы. Файловый резедентный вирус.

43. Вредоносное программное обеспечение. Компьютерные вирусы. Бутовый вирус.

44. Вредоносное программное обеспечение. Компьютерные вирусы. Макровирус.

45. Вредоносное программное обеспечение. Троянские программы. Семейства троянских программ.

46. Вредоносное программное обеспечение. Компьютерные вирусы. Компьютерные сетевые черви.

47. Вредоносное программное обеспечение. Компьютерные вирусы. Отличительные признаки компьютерных вирусов, троянских программ, компьютерных сетевых червей.

48. Вредоносное программное обеспечение. Другое вредоносное программное обеспечение. Примеры.

49. Средства борьбы с вредоносным программным обеспечением. Выполняемые функции.

50. Современные антивирусные пакеты.

Примерный перечень вопросов для зачета:

1. Общие понятия информационной безопасности компьютерных систем (ИБКС). Практические аспекты ИБКС, уровни обеспечения ИБКС.
2. Законодательный уровень обеспечения ИБКС. Основные законодательные акты и нормативные документы.
3. Административный уровень обеспечения ИБКС. Его назначение и содержание.
4. Процедурный уровень обеспечения ИБКС. Его назначение и содержание.
5. Программно-технический уровень обеспечения ИБКС. Его назначение и содержание.
6. Таксономия критериев информационной безопасности по «Оранжевой книге». Содержание понятия «ПОЛИТИКА БЕЗОПАСНОСТИ», и механизмы ее реализации.
7. Таксономия критериев информационной безопасности по «Оранжевой книге». Механизмы «ПРОИЗВОЛЬНОЕ УПРАВЛЕНИЕ ДОСТУПОМ», и «ПОВТОРНОЕ ИСПОЛЬЗОВАНИЕ ОБЪЕКТОВ».
8. Таксономия критериев информационной безопасности по «Оранжевой книге». Механизмы «МЕТКИ БЕЗОПАСНОСТИ», и «НОРМАТИВНОЕ УПРАВЛЕНИЕ ДОСТУПОМ».
9. Таксономия критериев информационной безопасности по «Оранжевой книге». Содержание понятия «АУДИТ», и механизмы его реализации.
10. Таксономия критериев информационной безопасности по «Оранжевой книге». Содержание понятия «КОРРЕКТНОСТЬ». Корректность на этапе функционирования и механизмы её реализации.
11. Таксономия критериев информационной безопасности по «Оранжевой книге». Содержание понятия «КОРРЕКТНОСТЬ». Корректность на этапе разработки и механизмы её реализации.
12. Таксономия критериев информационной безопасности по «Оранжевой книге». Содержание понятия «ДОКУМЕНТАЦИЯ».
13. Противодействие межсетевому несанкционированному доступу. Эталонная модель взаимодействия открытых систем. Назначение, принцип функционирования.
14. Противодействие межсетевому несанкционированному доступу. Комплексный межсетевой экран. Состав, назначение.

15. Противодействие межсетевому несанкционированному доступу. Экранирующий маршрутизатор. Назначение, выполняемые функции, достоинства и недостатки.
16. Противодействие межсетевому несанкционированному доступу. Шлюз сеансового уровня. Назначение, выполняемые функции, достоинства и недостатки.
17. Противодействие межсетевому несанкционированному доступу. Прикладной шлюз. Назначение, выполняемые функции, достоинства и недостатки.
18. Вредоносное программное обеспечение; виды, отличительные особенности.
19. Компьютерные вирусы. Файловый нерезидентный вирус.
20. Компьютерные вирусы. Файловый резидентный вирус.
21. Компьютерные вирусы. Бутовый вирус.
22. Компьютерные вирусы. Макровирусы. Скриптовые вирусы.
23. Вредоносное программное обеспечение. Троянские программы.
24. Вредоносное программное обеспечение. Сетевые черви.
25. Классификация средств борьбы с вредоносным программным обеспечением.
26. Технологии обнаружения вредоносного программного обеспечения, применяемые в современных средствах борьбы с ВПО.
27. Рекомендации по организации защиты от воздействия вредоносного ПО на информационные ресурсы предприятий.
28. Что регулирует Федеральный Закон РФ от 26.07.2017 № 187 «О безопасности критической информационной инфраструктуры Российской Федерации».
29. Понятие субъекта КИИ. Как определить принадлежность организации (предприятия, учреждения и т. п.) к субъектам КИИ.
30. Понятие объекта КИИ, и их классификация.
31. ГосСОПКА. Необходимость создания. Структура системы. Функции центров ГосСОПКА.
32. Роль и место НКЦКИ в структуре ГосСОПКА. Функции центра.
33. Порядок категорирования объектов КИИ, согласно требованиям ПП РФ от 8 февраля 2018 года № 127 «Об утверждении правил категорирования объектов КИИ РФ, а также Перечня показателей критериев значимости объектов КИИ РФ». Показатели критериев значимости.
34. Силы и средства обеспечения безопасности значимых объектов КИИ.
35. Требования к программным и программно-аппаратным средствам защиты ЗОКИИ.
36. Организационно-технические меры защиты объектов КИИ. Идентификация и аутентификация.
37. Организационно-технические меры защиты объектов КИИ. Управление доступом. Ограничение программной среды. Защита машинных носителей информации.

38. Организационно-технические меры защиты объектов КИИ. Аудит. Антивирусная защита.
39. Организационно-технические меры защиты объектов КИИ. Предотвращение вторжений. Обеспечение целостности. Обеспечение доступности.
40. Организационно-технические меры защиты объектов КИИ. Защита технических средств и систем. Защита информационной (автоматизированной) системы и ее компонентов.
41. Организационно-технические меры защиты объектов КИИ. Реагирование на компьютерные инциденты. Управление конфигурацией.
42. Организационно-технические меры защиты объектов КИИ. Управление обновлениями программного обеспечения.
43. Организационно-технические меры защиты объектов КИИ. Планирование мероприятий по обеспечению безопасности.
44. Организационно-технические меры защиты объектов КИИ. Обеспечение действий в нештатных ситуациях. Информирование и обучение персонала.
45. Классификация типовых угроз информации.
46. Оценка угроз информационной безопасности.

10. Методические рекомендации для обучающихся по освоению дисциплины

Методика преподавания дисциплины «Информационная безопасность» характеризуется совокупностью методов, приемов и средств обучения, обеспечивающих реализацию содержания и учебно-воспитательных целей дисциплины, которая может быть представлена как некоторая методическая система, включающая методы, приемы и средства обучения. Такой подход позволяет более качественно подойти к вопросу освоения дисциплины обучающимися.

10.1. Методические рекомендации для обучающихся по освоению материалов лекционных занятий

Лекции являются одним из важнейших видов учебных занятий и составляют основу теоретической подготовки обучающихся по дисциплинам вообще и по дисциплине «Информационная безопасность» в частности. Будучи по содержанию теоретическими, прикладными и методическими, по данной дисциплине они являются *теоретическими*. По назначению: *вводными, тематическими* и *заключительными*.

Лекция имеет целью дать систематизированные основы научных знаний по дисциплине, раскрыть состояние и перспективы прогресса конкретной области науки и экономики, сконцентрировать внимание на наиболее сложных и узловых вопросах. Эта цель определяет дидактическое назначение лекции, которое заключается в том, чтобы ознакомить обучающихся с основным

содержанием, категориями, принципами и закономерностями изучаемой темы и предмета обучения в целом, его главными идеями и направлениями развития, его прикладной стороной.

На лекции формируется научное мировоззрение будущего специалиста, закладываются теоретические основы фундаментальных знаний будущего управленца, стимулируется его активная познавательная деятельность, решается целый ряд вопросов воспитательного характера.

Методика преподавания лекционного курса дисциплины строится на использовании конкретной, оптимальной для нее методической системы. Методическая системы есть сумма методов, приемов и средств обучения. Основой для построения системы служат дидактические принципы высшей школы, педагогическая психология и обобщенный опыт преподавания дисциплины. При проведении лекций преподаватель опирается на базовые знания студентов по общенаучным дисциплинам, с тем, чтобы основное время уделить специфическим вопросам дисциплины, а не повторению материала по менеджменту, информатике и т.д. В процессе подготовки к лекции и в ходе ее изложения важным является развитие интереса обучающихся к преподаваемой дисциплине.

Интерес к изучению учебного материала достигается на лекции применением *комплекса методических приемов:* четкой формулировкой темы, разъяснением важности знания учебного материала для дальнейшей практической деятельности; выделением в изучаемом материале главного; созданием на занятиях хорошего эмоционального настроя; использованием творческого характера заданий на самостоятельную работу, выдаваемых обучающимся.

Вводная часть лекции (объявление темы, учебных вопросов и литературы, контрольный опрос) занимает около 10 минут. Темп ее изложения, как правило, выше темпа изложения основного содержания, что заставляет обучающихся собраться и сосредоточиться. Тщательная подготовка и отбор каждого слова начала лекции – необходимое условие успеха лекции вообще.

Способы чтения лекций.

Используются несколько способов чтения лекции: пересказ содержания лекции наизусть, без каких-либо конспектов; чтение по тексту; свободное выступление на основе конспекта (текста) лекции.

Темп лекции.

Так как в лекциях по дисциплине диктуются определения и формулировки, требующие дословного воспроизведения, то темп определяется способностью обучающихся сокращенно, но точно, полностью записать текст при неоднократном повторении его преподавателем.

Доступность для восприятия.

Она определяется через элементы обратной связи:

- замедленность действий обучающихся;
- неуверенность в конспектировании;
- ожидание дополнительных пояснений;
- вопросы с мест.

Принцип наглядности.

Использование приемов, позволяющих наглядно представлять обучаемым процессы, свойства предметов и т.д.

Эмоциональность изложения.

Одним из важнейших требований к лекции является эмоциональность изложения материала. Лектор должен читать лекцию с искренней убежденностью, хорошо владеть дикцией, интонацией и жестами, приводить яркие примеры и образные сравнения, которые вызывали бы у аудитории живой интерес. Все это должно быть хорошо продумано, прорепетировано, согласовано с содержанием лекции.

Методы предъявления учебного материала.

Лектору необходимо знать методы предъявления учебного материала при помощи учебной доски, плакатов и ТСО.

Повышению эффективности лекции способствуют хорошо подобранные иллюстрации (схемы, плакаты, кинофрагменты, слайды и др.), позволяющие быстрее и доходчивее раскрыть сущность излагаемых вопросов. Однако объем иллюстративного материала не должен быть чрезмерным, чтобы не рассеивать внимание обучаемых.

Активизация деятельности обучаемых.

Лекция предназначена не только и не столько для сообщения какой-то информации, а, в первую очередь, для развития мышления обучаемых. Одним из способов, активизирующих мышление, является такое построение изложения учебного материала, когда обучающиеся слушают, запоминают и конспектируют излагаемый лектором учебный материал, и вместе с ним участвуют в решении проблем, задач, вопросов, в выявлении рассматриваемых явлений. Такой методический прием получил название *проблемного изложения*.

Активизации мышления способствует рассмотрение в ходе лекции примеров и опыта передовых компаний. Подобные хорошо продуманные примеры помогают лучше усвоить содержание теоретических вопросов. Активность обучающихся на занятии зависит от того, насколько быстро и прочно установлен контакт преподавателя с обучаемыми. Это достигается: выдачей интересной справки об ученых, работающих над данной темой, или рассказ об ее предыстории; постановкой интересного вопроса или захватывающей задачи, решению которых будет посвящено данное учебное занятие и т.д.

Энергичное начало учебного занятия – хорошая предпосылка для его успешного проведения. Но этого недостаточно. Важно удержать интерес и внимание аудитории к изучаемому материалу в ходе всего учебного занятия. Это достигается установлением контактов с аудиторией с использованием элементов беседы (Понятно? Ясно? Как вы думаете? Каким образом?).

Подготовленные и читаемые лекции требуют постоянного совершенствования: обновления содержания лекционного курса, учета последних достижений науки, теории и практики, изыскания новых, более эффективных приемов и способов изложения учебного материала, а также средств иллюстрации.

10.2 Методические рекомендации для обучающихся по освоению материалов практических занятий

Практическое занятие проводится в целях выработки практических умений и приобретения навыков при решении управленческих задач.

Главным содержанием этих занятий является практическая работа каждого студента, форма занятия – групповая, а основной метод, используемый на занятии – метод практической работы.

В дидактической системе изучения дисциплины практические занятия стоят после лекций. Таким образом, дидактическое назначение практических занятий – закрепление, углубление и комплексное применение теоретических знаний, выработка умений и навыков обучающихся в решении практических задач. Вместе с тем, на этих занятиях, осуществляется активное формирование и развитие навыков и качеств, необходимых для последующей профессиональной деятельности.

В зависимости от специфики преподаваемых дисциплин практические занятия условно можно разделить на две группы. Основным содержанием первой группы занятий является решение задач, производство расчетов, разработка документов, выполнение графических и других работ, второй группы – овладение методикой анализа и принятия решений.

Методика подготовки и проведения практических занятий по различным учебным дисциплинам весьма разнообразна и конкретно рассматривается в частных методиках преподавания. В то же время в ней можно выделить некоторые общие приемы и способы, характерные для всех или группы дисциплин.

Любое практическое занятие начинается, как правило, с формулирования его целевых установок. Понимание обучаемыми целей и задач занятия, его значения для специальной подготовки способствует повышению интереса к занятию и активизации работы по овладению учебным материалом. Вслед за этим производится краткое рассмотрение основных теоретических положений, которые являются исходными для работы обучаемых на данном занятии. Обычно это делается в форме опроса обучаемых, который служит также средством контроля за их самостоятельной работой. Обобщение вопросов теории может быть поручено также одному из обучаемых. В этом случае соответствующее задание дается заранее всей учебной группе, что служит дополнительным стимулом в самостоятельной работе. В заключении преподаватель дает оценку ответов обучаемых и приводит уточненную формулировку теоретических положений.

Основную часть практического занятия составляет работа обучаемых по выполнению учебных заданий под руководством преподавателя. Эффективность этой части занятия зависит от ряда условий. Прежде всего, требуется тщательная разработка учебных заданий. По своему содержанию каждое задание должно быть логическим развитием основной идеи дисциплины и учитывать специальность подготовки обучаемых. Наряду с этим в задании необходимо предусмотреть использование и закрепление знаний,

навыков и умений, полученных при изучении смежных дисциплин, т.е. учесть принцип комплексности в обучении.

Практические занятия, закрепляя и углубляя знания, в то же время должны всемерно содействовать развитию мышления обучаемых. Наиболее успешно это достигается в том случае, когда учебное задание содержит элементы проблемности, т.е. возможность неоднозначных решений или ответов, побуждающих обучаемых самостоятельно рассуждать, искать ответы и т.п. Постановка на занятиях проблемных задач и вопросов требует соответствующей подготовки преподавателя. Готовясь к занятию, он должен заранее наметить все вопросы, имеющие проблемный характер, продумать четкую их формулировку и оптимальные варианты решения с активным участием обучаемых.

На практических занятиях благоприятные условия складываются для индивидуализации обучения. При проведении занятий преподаватель имеет возможность наблюдать за работой каждого обучаемого, изучать их индивидуальные особенности, своевременно оказывать помощь в решении возникающих затруднений. Наиболее успешно выполняющим задание преподаватель может дать дополнительные вопросы, а отстающим уделить больше внимания, как на занятии, так и во внеучебное время.

При возникновении у аудитории общих неясных вопросов преподаватель может разъяснить их с использованием классной доски, однако при этом он не должен повторять лекционный материал или повторно решать задачи и примеры, приведенные на лекции. Во всех случаях педагогически неоправданно решение задач на доске преподавателем или обучаемыми в течение всего занятия, так как оно не способствует развитию самостоятельности и ведет к пассивной работе большинства обучаемых.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 25.04.04 Эксплуатация аэропортов и обеспечение полетов воздушных судов.

Программа рассмотрена и утверждена на заседании кафедры №12 «Радиоэлектронных систем» «25» мая 2021 г., протокол № 8.

Разработчики:

д.т.н., ст.н.с. Кудряков С.А.
(ученая степень, ученое звание, фамилия и инициалы заведующего кафедрой)

старший преподаватель Шестаков С.А.
(ученая степень, ученое звание, фамилия и инициалы разработчиков)

Заведующий кафедрой № 12:

д.т.н., ст.н.с. Кудряков С.А.
(ученая степень, ученое звание, фамилия и инициалы заведующего кафедрой)

Директор Высшей школы аэронавигации:

к.т.н. Богданов В.Г.
(ученая степень, ученое звание, фамилия и инициалы директора Высшей школы аэронавигации)

Программа согласована:

Руководитель ОПОП ВО:

к.т.н. Коникова Е.В.
(ученая степень, ученое звание, фамилия и инициалы руководителя ОПОП)

Программа рассмотрена и одобрена на заседании Учебно-методического совета Университета 16 июня 2021 г., протокол № 7.