Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 08.08.2024 15:35:44
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Декан факультета
«Информационные технологии»
_____ / Д.Г.Демидов /
«15» февраля 2024г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Кибербезопасность роботизированных беспилотных систем и комплексов

Направление подготовки
27.04.04 Управление в технических системах

Образовательная программа (профиль подготовки)
«Беспилотная робототехника»

Квалификация (степень) выпускника
Магистр

Форма обучения
Очная

Год приема – 2024

Москва 2024 г.

Рабочая программа составлена на основе ФГОС ВО и учебного плана Московского политехнического университета по направлению (специальности) 27.04.04 Управление в технических системах, по профилю подготовки Беспилотная робототехника

Разработчик(и):

к. ф.-м. н., доцент кафедры  / Т.Т. Идиатуллов /

Согласовано:
Заведующий кафедрой «СМАРТ-технологии»,
к.т.н., доцент  / Е.В. Петрунина /

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине 4
2 Место дисциплины в структуре образовательной программы .... **Ошибка! Закладка не определена.**
3 Структура и содержание дисциплины ..... **Ошибка! Закладка не определена.**
3.1 Виды учебной работы и трудоемкость ..... **Ошибка! Закладка не определена.**
3.2 Тематический план изучения дисциплины ..... **Ошибка! Закладка не определена.**
3.3 Содержание дисциплины ..... **Ошибка! Закладка не определена.**
3.4 Тематика семинарских/практических и лабораторных занятий **Ошибка! Закладка не определена.**
3.5 Тематика курсовых проектов (курсовых работ). **Ошибка! Закладка не определена.**
4 Учебно-методическое и информационное обеспечение ..... **Ошибка! Закладка не определена.**
4.1 Нормативные документы и ГОСТы ..... **Ошибка! Закладка не определена.**
4.2 Основная литература ..... **Ошибка! Закладка не определена.**
4.3 Дополнительная литература ..... **Ошибка! Закладка не определена.**
4.4 Электронные образовательные ресурсы ..... **Ошибка! Закладка не определена.**
4.5 Лицензионное и свободно распространяемое программное обеспечение .... **Ошибка! Закладка не определена.**
4.6 Современные профессиональные базы данных и информационные справочные системы ..... **Ошибка! Закладка не определена.**
5 Материально-техническое обеспечение ..... **Ошибка! Закладка не определена.**
5.1 Требования к оборудованию и помещению для занятий ..... **Ошибка! Закладка не определена.**
5.2 Требования к программному обеспечению ..... **Ошибка! Закладка не определена.**
6 Методические рекомендации ..... **Ошибка! Закладка не определена.**
6.1 Методические рекомендации для преподавателя по организации обучения **Ошибка! Закладка не определена.**
6.2 Методические указания для обучающихся по освоению дисциплины ..... **Ошибка! Закладка не определена.**
7 Фонд оценочных средств ..... **Ошибка! Закладка не определена.**
7.1 Методы контроля и оценивания результатов обучения ..... **Ошибка! Закладка не определена.**
7.2 Шкала и критерии оценивания результатов обучения ..... **Ошибка! Закладка не определена.**
7.3 Оценочные средства ..... **Ошибка! Закладка не определена.**
Приложение 20

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Кибербезопасность роботизированных беспилотных систем и комплексов» относится:

- знакомство студентов с методами и подходами обеспечением кибербезопасности;
- формирование навыков разработки механизмов обеспечения кибербезопасности РБСк;
- формирование у студентов навыков поддержки кибербезопасности РБС;
- закрепление получаемых в семестре знаний и навыков на практике;
- подготовка студентов к деятельности в соответствии с квалификационной характеристикой магистра.

К **основным задачам** дисциплины относятся:

- ознакомление студента с подходами и методами обеспечением кибербезопасности;
- формирование у студента навыков разработки механизмов кибербезопасности;
- ознакомление студента с синтезом и настройкой систем управления бехопасностью РБС.

Обучение по дисциплине «Кибербезопасность роботизированных беспилотных систем и комплексов» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	**Индикаторы достижения компетенции**
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**УК-1.1. Знает:** процедуры критического анализа, методики анализа результатов исследования и разработки стратегий проведения исследований, организации процесса принятия решения **УК-1.2. Умеет:** принимать конкретные решения для повышения эффективности процедур анализа проблем, принятия решений и разработки стратегий **УК-1.3. Владеет:** методами установления причинно-следственных связей и определения наиболее значимых среди них; методиками постановки цели и определения способов ее достижения; методиками разработки стратегий действий при проблемных ситуациях
ПК-2. Проектирование АСУП	**ИПК 2.1. Знает:** основные понятия

	в области автоматизированных систем управления производством; цели проектирования АСУП; основные алгоритмы и методы решения задач АСУП; прикладные программы управления проектами: наименования, возможности и порядок работы в них; методы планирования и организации работ в организации; прикладные компьютерные программы для вычислений: наименования, возможности и порядок работы в них; требования к структуре, содержанию и оформлению технического задания на создание АСУП; методики расчета технико-экономического обоснования необходимости создания АСУП **ИПК 2.2. Умеет:** выявлять элементы системы управления, нуждающиеся в автоматизации; устанавливать цели при проектировании АСУП; выделять основные задачи при проектировании АСУП; разрабатывать концепцию АСУП организации; составлять план создания и внедрения АСУП, определять сроки выполнения работ, определять назначенные ресурсы с использованием прикладных программ управления проектами **ИПК 2.3. Владеет:** методами: разработки вариантов концепции АСУП и выбор варианта концепции, удовлетворяющего требованиям пользователей; расчета экономической эффективности внедрения АСУП; определения планируемых свойств АСУП (эффективности, совместимости, адаптивности, надежности, живучести); разработки технического задания на создание АСУП; выбора типовых решений

	компонентов АСУП или обоснование необходимости разработки оригинальных решений; разработки плана создания и внедрения АСУП; проектирования информационной модели интегрированной АСУП

Дисциплина относится к факультативной части.

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП:

- Анализ и обработка данных;
- Искусственные нейронные сети;
- Теория автоматического управления;
- Системы технического зрения в беспилотной робототехнике;
- Задачи планирования движения и навизация;
- Учебная (ознакомительная) практика;
- Учебная (проектно-технологическая) практика;
- Производственная (проектно-технологическая) практика;
- Производственная (НИР) практика.

.

2. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, т.е. 72 академических часов (из них 36 часов – самостоятельная работа студентов).

На втором курсе, **в треьем** семестре выделяется 2 зачетных единицы, т.е. 72 академических часа (из них 36 часов – самостоятельная работа студентов).

Разделы дисциплины «Системы связи и мониторинга роботизированных транспортных комплексов» изучаются на втором курсе в четвертом семестре.

Форма рубежного контроля по дисциплине – экзамен.

Структура и содержание дисциплины «Кибербезопасность роботизированных беспилотных систем и комплексов» по срокам и видам работы отражены в Приложении 1.

3.1. Виды учебной работы и трудоемкость (по формам обучения)

Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры
			3
1	Аудиторные занятия	36	36
	В том числе:		
1.1	Лекции	18	18
1.2	Семинарские/практические занятия		
1.3	Лабораторные занятия	18	18
2	Самостоятельная работа	36	36
	В том числе:		
2.1	Выполнение самостоятельных практических занятий	36	36
2.2	Тестирование		
3	Промежуточная аттестация		
	Зачет		
	Итого:	72/2	72/2

3.2. Тематический план изучения дисциплины (по формам обучения)

Очная форма обучения

/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/практические занятия	Лабораторные занятия	Практическая подготовка	
	Тема 1. Введение. Основные понятия и принципы обеспечения кибербезопасности РБС		2		2		4
	Тема 2. Теоретические и практические основы кибербезопасности и киберустойчивости.		2		2		4
	Тема 3. Подходы к созданию современных приложений для БРС		2		2		4
	Тема 4. Методологии разработки DevOps и DevSecOps.		4		4		8
	Тема 5. Уровни безопасности. Матрицы угроз. Политика безопасности.		4		4		8
	Тема 6. Лучшие практики для обеспечения кибербезопасности и киберустойчивости.		4		4		4
Итого			**18**		**18**		**26**

3.3 Содержание дисциплины

Тема 1. Введение. Основные понятия и принципы обеспечения кибербезопасности РБС

Основные термины и определения. Кибербезопасность. Практики кибербезопасности. Атака, уязвимость, матрица угроз. Политика безопасности. Риски. Угрозы кибербезопасности. Оценка. Тактики и техники злоумышленников

Тема 2. Теоретические и практические основы кибербезопасности и киберустойчивости.

Кибербезопасность. Киберустойчивость. Техники обеспечения киберустойчивости. Совокупность организационных, технических, программно-аппаратных, морально-этических мер. Тактические принципы обеспечения киберустойчивости.

Тема 3. Подходы к созданию современных приложений

Подход к созданию приложений в средах облачных вычислений (Cloud Native). Cloud Native архитектура. Методология создания приложений «программное обеспечение как услуга (The Twelve-Factor App).

Тема 4. Методологии разработки DevOps и DevSecOps.

Методология разработки DevOps. GitOps методология, Методология разработки DevSecOps

Тема 5. Уровни безопасности. Матрицы угроз. Политика безопасности

Матрицы угроз. Политика безопасности. Уровни безопасности. Тезнические меры. Организационные меры обеспечения кибербезопасности.

Тема 6. Лучшие практики для обеспечения кибербезопасности и киберустойчивости.

Модель безопасности Нулевое доверие. ZTNA (Zero Trust Network Access) основная технология, связанная с архитектурой Zero Trust. Разбор инцидентов безопасности. Постмортем (postmortem). Программные , аппаратные меры обеспечения безопасности БРС.

3. 3. Тематика семинарских/практических и лабораторных занятий

Лабораторные работы

Лабораторная работа №1 «Настройка системы контроля версий и автоматизация сборки приложений»

Лабораторная работа №2 «.Изучение протоколов передачи данных в сети,

инструментов и индикаторов активности. Задачи 1. выполнить набор действий по передаче информации и файлов между несколькими виртуальными машинами с использованием протоколов и инструментов: SSH, Telnet, FTP, SFTP, SMB» Лабораторная работа №3 «изучение принципов анализа защищенности k8s инфраструктуры. Задачи 1. изучить основы концепций k8s и Docker;.»

Для проведения лабораторных работ требуется компьютерный класс. объеденный в локальную сеть с выходом в Интернет. Компьютеры должны быть объединены локальной сетью. Необходим выход в глобальную сеть Интернет. Требуемое программное обеспечением: компилятор языка Python, текстовый редактор, офисный пакет LibreOffice.

Компьютерный класс должен иметь возможность обновления и установки дополнительного свободно распространяемого программного обеспечения.

3.2 Тематика вопросов для самостоятельного изучения

• Изучение тенденции развития научных исследований в выбранной области..
• Изучение методов работы с электронными библиотеками.
• Изучение методов коллективной разработки НИР.
• Изучение средств автоматизированной подачи заявок н гранты. Патентный поиск.

4. Учебно-методическое и информационное обеспечение

4.1Нормативные документы и ГОСТы

1. ГОСТ 21552-84 СРЕДСТВА ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение.
2. ГОСТ Р 43.0.12-2018 Базы знаний в технической деятельности.
3. ГОСТ Р 57321.2-2018 Менеджмент знаний. Менеджмент знаний в области инжиниринга. Часть 2. Проектирование на основе баз знаний.
4. ГОСТ Р 43.0.28-2022 Информационное обеспечение техники и операторской деятельности. Базы знаний в интеллектуализации деятельности.
5. ГОСТ Р 59869-2021 Интеллектуальные системы обучения. Общие положения.

4.2 Основная литература

1. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL:

http://biblioclub.ru/index.php?page=book&id=438331

2. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

3. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях: учебник ипрактикум для вузов / М. В. Дибров. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 423 с. — (Высшее образование). — ISBN 978-5-534-16546-3. — Текст:электронный // Образовательная платформа Юрайт [сайт]. — URL:https://urait.ru/bcode/531273 (дата обращения: 18.09.2023)

4.3 Дополнительная литература

1. Трофимов, В. В. Глобальные и локальные сети: учебник для вузов / В. В. Трофимов, М. И. Барабанова, В. И. Кияев. — 4-е изд., перераб. и доп. — Москва: Издательство Юрайт,2023. — 162 с. — (Высшее образование). — ISBN 978-5-534-17504-2. — Текст: электронный// Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/533206 (датаобращения: 18.09.2023)

2. Замятина, О. М. Вычислительные системы, сети и телекоммуникации.
Моделирование сетей: учебное пособие для вузов / О. М. Замятина. — Москва: Издательство Юрайт, 2023. — 167 с. — (Высшее образование). — ISBN 978-5-534-16305-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530772 (дата обращения: 18.09.2023).

3.Тяпкин, В.Н. Методы определения навигационных параметров подвижных средств с использованием спутниковой радионавигационной системы ГЛОНАСС [Электронный ресурс]: монография / В.Н. Тяпкин, Е.Н. Гарин. – Красноярск: Сиб. федер. ун-т, 2012. – 260 с. // ZNANIUM.COM: электронно-библиотечная система. – Режим доступа: http://znanium.com/bookread2.php?book=442662,

4. Афонин, А.А. Микропроцессорная техника в приборах, системах и комплексах ориентации, навигации и управления летательных аппаратов [Электронный ресурс] : учебное пособие к лабораторным работам / А.А. Афонин, Г.Г. Ямашев. – Электрон. текстовые данные. – Саратов: Ай Пи Эр Медиа, 2015. – 143 с.

Электронные образовательные ресурсы

1. ЭОР в разработке.

4.4 Лицензионное и свободно распространяемое программное обеспечение

1. Среда разработки Microsoft VisualStudio с установленным пакетом расширения языка Python
3. Офисный пакет Libre Office или Microsoft Office

4.5 Современные профессиональные базы данных и информационные справочные системы

1. Справочно-правовая системы «КонсультантПлюс: Некоммерческая интернетверсия» https://www.consultant.ru/online/
2. Официальный интернет-портал правовой информации http://pravo.gov.ru
3. Российская национальная библиотека http://www.nlr.ru
4. ЭБС «Университетская библиотека онлайн» https://biblioclub.ru/index.php
5. Единое окно доступа к образовательным ресурсам Федеральный портал http://window.edu.ru
6. Научная электронная библиотека http://www.elibrary.ru
7. Российская государственная библиотека http://www.rsl.ru

5 Материально-техническое обеспечение

1. Компьютерные классы с оснащением: столы, стулья, аудиторная доска, использование переносного мультимедийного комплекса (переносной проектор, персональный ноутбук).
2. Персональные компьютеры, мониторы, мышки, клавиатуры. Рабочее место преподавателя: стол, стул.
3. Аудитория для самостоятельной работы.
4. Библиотека, читальный зал.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.
2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.
3. При организации и проведения экзаменов в практико-ориентированной форме следует использовать утвержденные кафедрой Методические рекомендации.

6.2 Методические указания для обучающихся по освоению дисциплины

Получение углубленных знаний по дисциплине достигается за счет активной самостоятельной работы обучающихся. Выделяемые часы целесообразно использовать для знакомства с учебной и научной литературой по проблемам

дисциплины, анализа научных концепций.

Промежуточная аттестация обучающихся в форме зачѐта проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине проводится преподавателем, ведущим занятия по дисциплине методом экспертной оценки. По итогам промежуточной аттестации по дисциплине выставляется оценка «отлично», «хорошо», «удовлетворительно» или «не удовлетворительно».

К промежуточной аттестации допускаются только обучающиеся, выполнившие все виды учебной работы, предусмотренные рабочей программой по дисциплине «Искусственные нейронные сети».

6.3 Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья: - создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;
- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников, например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения аудиально;
- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и ассимиляционных технологий;
- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;
- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;
- увеличение продолжительности сдачи обучающимся инвалидом или лицом

с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи: - продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут; - продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;

- продолжительности выступления, обучающегося при защите курсовой работы - не более чем на 15 минут.

Для обеспечения подготовки людей в формате очной аудиторной работы с ограниченными возможностями движения выбираются аудитории с доступностью в рамках требований по организации безбарьерной среды движения.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю).

Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
ПК-2. Способен исследовать, разрабатывать и эксплуатировать средства и системы автоматизации и управления различного назначения, в том числе жизненным циклом продукции и ее качеством				
Знает основные понятия в области автоматизированных систем управления производством; цели проектирования АСУП; основные алгоритмы и методы решения задач АСУП; прикладные программы	Обучающийся демонстрирует полное отсутствие знаний основ в области автоматизированных систем управления производством; цели проектирования АСУП; основные алгоритмы и методы решения задач АСУП;	Обучающийся демонстрирует неполное соответствие знаний основ в области автоматизированных систем управления производством; цели проектирования АСУП; основные алгоритмы и методы решения задач АСУП;.Допускаются значительные ошибки,	Обучающийся демонстрирует частичное соответствие знаний основных принципов основ и методов в области автоматизированных систем управления производством; цели проектирования АСУП; основные алгоритмы и методы решения задач	Обучающийся демонстрирует полное соответствие знаний основ и методов в области автоматизированных систем управления производством; цели проектирования АСУП; основные алгоритмы и методы решения задач АСУП; Свободно оперирует

управления проектами: наименования, возможности и порядок работы в них; методы планирования и организации работ в организации; прикладные компьютерные программы для вычислений: наименования, возможности и порядок работы в них; требования к структуре, содержанию и оформлению технического задания на создание АСУП; методики расчета технико-экономического обоснования необходимости		проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	АСУП;.Допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	приобретенными знаниями.

создания АСУП				
Умеет выявлять элементы системы управления, нуждающиеся в автоматизации; устанавливать цели при проектировании АСУП; выделять основные задачи при проектировании АСУП; разрабатывать концепцию АСУП организации; составлять план создания и внедрения АСУП, определять сроки выполнения работ, определять назначенные ресурсы с использованием	Обучающийся не умеет выявлять элементы системы управления, нуждающиеся в автоматизации; устанавливать цели при проектировании АСУП; выделять основные задачи при проектировании АСУП; разрабатывать концепцию АСУП организации;	Обучающийся демонстрирует неполное соответствие следующих умений: выявлять элементы системы управления, нуждающиеся в автоматизации; устанавливать цели при проектировании АСУП; выделять основные задачи при проектировании АСУП; разрабатывать концепцию АСУП организации; Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения	Обучающийся демонстрирует частичное соответствие следующих умений: выявлять элементы системы управления, нуждающиеся в автоматизации; устанавливать цели при проектировании АСУП; выделять основные задачи при проектировании АСУП; разрабатывать концепцию АСУП организации; Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на	Обучающийся демонстрирует полное соответствие следующих умений: выявлять элементы системы управления, нуждающиеся в автоматизации; устанавливать цели при проектировании АСУП; выделять основные задачи при проектировании АСУП; разрабатывать концепцию АСУП организации; Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.

прикладных программ управления проектами		при оперировании умениями при их переносе на новые ситуации.	новые, нестандартные ситуации.	
Владеет: **методами:** разработки вариантов концепции АСУП и выбор варианта концепции, удовлетворяющего требованиям пользователей; расчета экономической эффективности внедрения АСУП; определения планируемых свойств АСУП (эффективности, совместимости, адаптивности, надежности, живучести); разработки технического задания на создание АСУП; выбора	Обучающийся не владеет навыками разработки вариантов концепции АСУП и выбор варианта концепции, удовлетворяющего требованиям пользователей; расчета экономической эффективности внедрения АСУП; определения планируемых свойств АСУП (эффективности,	Обучающийся в неполном объеме владеет навыками разработки вариантов концепции АСУП и выбор варианта концепции, удовлетворяющего требованиям пользователей; расчета экономической эффективности внедрения АСУП; определения планируемых свойств АСУП (эффективности,. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет навыками разработки вариантов концепции АСУП и выбор варианта концепции, удовлетворяющего требованиям пользователей; расчета экономической эффективности внедрения АСУП; определения планируемых свойств АСУП (эффективности,.. Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные	Обучающийся в полном объеме владеет навыками разработки вариантов концепции АСУП и выбор варианта концепции, удовлетворяющего требованиям пользователей; расчета экономической эффективности внедрения АСУП; определения планируемых свойств АСУП (эффективности, Свободно применяет полученные навыки в ситуациях повышенной сложности.

типовых решений компонентов АСУП или обоснование необходимости разработки оригинальных решений; разработки плана создания и внедрения АСУП; проектирования информационной модели интегрированной АСУП			ситуации.	

7.2 Шкала и критерии оценивания результатов обучения (зачет).

Форма промежуточной аттестации: зачет.
Обязательными условиями подготовки студента к промежуточной аттестации является выполнение и защита студентом лабораторных работ, предусмотренных рабочей программой.

Шкала оценивания	Описание
Зачтено	Достигнуты пороговые значения для формируемых на момент проведения аттестации уровней компетенций. Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Не зачтено	Не достигнуто пороговое значение хотя бы для одного уровня формируемых на момент проведения аттестации компетенций. Не выполнен один или более видов учебной

	работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средств представлены в Приложении к рабочей программе

7.3 Оценочные средства

7.3.1 Текущий контроль

Текущий контроль выполняется путем выполнения и защиты лабораторных работ.

7.3.2 Промежуточная аттестация

Промежуточная аттестация может проводиться в форме тестирования или устного экзамена. Допуск до промежуточной аттестации выполняется после выполнения работ лабораторного практикума в полном объеме.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

«Кибербезопасность роботизированных беспилотных систем и комплексов»

1. КОНТРОЛЬНЫЕ ВОПРОСЫ К ДИСЦИПЛИНЕ

1. Жизненный цикл веб-приложений

2. Понятие и основные принципы обеспечения кибербезопасности и киберустойчивости

3. Инструменты логирования и анализа событий

4. Уязвимости и угрозы, оценка киберустойчивости и киберучения

5. Cloud native

6. Методология 12 factor apps

7. Упущенные факторы из методологии 12 factor app

8. DevOps

9. DevSecOps

10. Постмортем

11. Принцип нулевого доверия

12. Основные типы аудита безопасности информационных систем

13. Матрица MITRE ATT&CK, понятие killchain

14. Классификация уязвимостей и методы их оценки

15. Методы анализа исходных данных об исследуемом объекте

16. Сбор информации с использованием DNS

17. Методы сбора информации о персонале организации

18. Методы сканирования периметра 64

19. Основные протоколы прикладного уровня и их эксплуатация на периметре организации

20. Парольная политика и методы защиты от атак методом перебора

21. Анализ безопасности конфигураций веб-сервера

22. Анализ структуры веб-сервиса, предположение векторов атаки

23. Типичные уязвимости веб-сервисов

24. Автоматизированные средства эксплуатации уязвимостей

25. Типы операционных систем и их особенности

26. Виды удаленного доступа и способы его получения

27. Особенности закрепления в различных ОС

28. Способы сокрытия присутствия

29. Привилегии и методы их повышения

30. Туннелирование для перемещения по корпоративной сети

31. Прокси и принципы его функционирования

32. Основные методы атак с использованием социальной инженерии

33. Методы защиты от атак с использованием социальной инженерии

34. Tor и анонимизация в сети

35. Методы сокрытия тестирования на проникновение

2. ТИПОВОЕ ПРАКТИЧЕСКОЕ ЗАДАНИЕ

1. Методы защиты от атак с использованием социальной инженерии
2. Туннелирование для перемещения по корпоративной сети.
3. Парольная политика и методы защиты от атак методом перебора.
4. Методы сокрытия тестирования на проникновения