МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Луганский государственный университет имени Владимира Даля»

Институт гражданской защиты
Кафедра специальных технических средств

УТВЕРЖДАЮ
Директор института гражданской защиты
_____ Малкин В.Ю.
«07» февраля 2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«КИБЕРБЕЗОПАСНОСТЬ БАС»

По направлению подготовки 25.03.03 Аэронавигация
Профиль «Эксплуатация беспилотных авиационных систем»

Луганск 2024

Лист согласования РПУД

Рабочая программа учебной дисциплины «Кибербезопасность БАС» по направлению подготовки 25.03.03 Аэронавигация профиля «Эксплуатация беспилотных авиационных систем» – 24 с.

Рабочая программа учебной дисциплины «Кибербезопасность БАС» составлена с учетом Федерального государственного образовательного стандарта высшего образования по направлению подготовки 25.03.03 Аэронавигация (утвержденный приказом Министерства образования и науки Российской Федерации от 21.08.2020 г. № 1084).

СОСТАВИТЕЛИ:
к.т.н., доцент Сыровой Г.В.

Рабочая программа дисциплины утверждена на заседании кафедры специальные технические средства
«16» 01 2024 года, протокол № 1.

Заведующий кафедрой
специальных технических средств _____ Победа Т. В.

Переутверждена: «____» _____20___ г., протокол № _____

Согласована:
Директор Института гражданской защиты _____ В.Ю. Малкин
Переутверждена «____» _____20_____ года, протокол №_____

Рекомендована на заседании учебно-методической комиссии института гражданской защиты «06» 02 2024 года, протокол № 6.

Председатель учебно-методической комиссии
института гражданской защиты _____ Михайлов Д.В.

1. Цели и задачи освоения дисциплины (модуля)

Целью изучения дисциплины «Кибербезопасность БАС» является формирование у студентов знаний и практических навыков о методах и средствах обеспечения кибербезопасности беспилотных авиационных систем, как критически важных объектов инфраструктуры воздушного транспорта.

Задачами изучения дисциплины «Кибербезопасность БАС» являются:

- знание основ теории кибербезопасности полетов;
- понимание основных требований Стандартов и Рекомендуемой практики (SARPs) ИКАО и воздушного законодательства РФ в части управления кибербезопасностью полетов на государственном уровне и в авиапредприятиях;
- освоение методов сравнительного анализа передовых практик в области управления кибербезопасностью полетов в мировой гражданской авиации и их применимость для решения задач по эксплуатации БАС;
- получение практических навыков по кибербезопасности поддержанию СУБП в авиапредприятиях, эксплуатирующих БАС.

Дисциплина «Кибербезопасность БАС» обеспечивает подготовку выпускника к эксплуатационно-технологическому и сервисному виду профессиональной деятельности.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина «Кибербезопасность БАС» относится к части, формируемой участниками образовательных отношений модуля обязательных дисциплин учебного плана.

Необходимыми условиями для освоения дисциплины являются:

знания:

- цели и задачи обеспечения безопасности полетов;
- требования международных стандартов и рекомендуемые практики по обеспечению безопасности полетов;
- законодательство и нормативные правовые акты Российской Федерации в области безопасности полетов;
- показатели безопасности полетов воздушных судов;
- факторы, влияющие на безопасность полётов;
-терминологию, основные определения и формулировки, используемые при характеристике состояния безопасности полетов;

умения:

-соблюдать требования законодательства и нормативных правовых актов Российской федерации, международных стандартов и рекомендуемую практику Международной организации гражданской авиации, регламентирующие обеспечение безопасности полётов воздушных судов и использования воздушного пространства;

-выполнять мероприятия, направленные на обеспечения безопасности полетов воздушных судов, безопасности использования воздушного пространства;

владеть навыками:

-методами и процедурами обеспечения безопасности полетов воздушных судов и использования воздушного пространства;

- навыками применения законодательства и нормативных правовых актов Российской Федерации, международных стандартов и рекомендуемой практики в целях обеспечения безопасности полётов воздушных судов и использования воздушного пространства.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)

Код и наименование компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Перечень планируемых результатов
ПК-11. Способен проводить мероприятия по обеспечению безопасности на ВТ	ПК-11.1 принимает решение по управлению БВС СВТ с использованием знаний в области человеческого фактора; ПК-11.2 обнаруживает и реагирует на аварийные и необычные ситуации, связанные с операциями БВС, управлением в условиях ограниченной функциональности БВС и потери линии связи; ПК-11.3 участвует в проведении поисковых работ в случае аварийной посадки БВС СВТ.	*Знать:* - показатели безопасности полетов воздушных судов; - факторы, влияющие на безопасность полётов; -терминологию, основные определения и формулировки, используемые при характеристике состояния безопасности полетов; - принципы, методы и процедуры обеспечения безопасности полетов. *Уметь:* -выполнять мероприятия, направленные на обеспечения безопасности полетов воздушных судов, безопасности использования воздушного пространства; -применять законодательство и нормативно правовые акты Российской Федерации, в области безопасности полетов в профессиональной деятельности; -обеспечивать безопасность полетов воздушных судов. *Владеть:* -данными о состоянии безопасности полетов и безопасности использования воздушного пространства.

4. Структура и содержание дисциплины

4.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов (зач. ед.)**	
	Очная форма	**Заочная форма**
Общая учебная нагрузка (всего)	**108 (3,0 зач. ед.)**	**-**
Обязательная аудиторная учебная нагрузка (всего) в том числе:	**51**	**-**
Лекции	34	-

Семинарские занятия	-	-
Практические занятия	17	-
Лабораторные работы		
Курсовая работа (курсовой проект)	-	-
Другие формы и методы организации образовательного процесса (*расчетно-графические работы, групповые дискуссии, ролевые игры, тренинг, компьютерные симуляции, интерактивные лекции, семинары, анализ деловых ситуаций и т.п.)*	-	-
Самостоятельная работа студента (всего)	**57**	**-**
Форма аттестации	зачет	-

4.2 Содержание разделов дисциплины

Семестр 4

Тема 1. **Введение в кибербезопасность БПЛА**

В этой лекции рассматриваются основные понятия кибербезопасности и ее важность для беспилотных летательных аппаратов (БПЛА). Обсуждаются угрозы, с которыми сталкиваются БПЛА, включая кибератаки, вмешательство в управление и утечку данных. Студенты узнают о различных типах атак, таких как атаки "человек посередине" и DDoS-атаки. Также рассматриваются примеры реальных инцидентов, связанных с кибербезопасностью БПЛА. Лекция включает обсуждение нормативных актов и стандартов, регулирующих кибербезопасность в этой области. Важным аспектом является необходимость интеграции кибербезопасности на всех этапах жизненного цикла БПЛА. Студенты познакомятся с основными принципами защиты информации и систем. Лекция завершится обсуждением будущих тенденций в кибербезопасности БПЛА.

Тема 2. **Угрозы и уязвимости БПЛА**

В этой лекции рассматриваются основные угрозы и уязвимости, с которыми сталкиваются БПЛА. Студенты узнают о различных типах атак, включая физические, программные и сетевые. Обсуждаются уязвимости в системах управления, навигации и связи БПЛА. Лекция включает анализ примеров атак на БПЛА и их последствия. Также рассматриваются методы оценки уязвимостей и рисков. Студенты познакомятся с инструментами и методами тестирования на проникновение. Важным аспектом является необходимость постоянного мониторинга и обновления систем безопасности. Лекция завершится обсуждением стратегий минимизации рисков.

Тема 3. **Криптография и защита данных в БПЛА**

В этой лекции рассматриваются основы криптографии и ее применение для защиты данных БПЛА. Студенты узнают о различных методах шифрования, включая симметричное и асимметричное шифрование. Обсуждаются протоколы безопасности, такие как SSL/TLS, и их применение в системах БПЛА. Лекция включает примеры использования криптографии для защиты связи и хранения данных. Также рассматриваются вопросы управления ключами и аутентификации. Студенты познакомятся с современными стандартами криптографической защиты. Важным аспектом является необходимость соблюдения нормативных требований в области защиты данных. Лекция завершится обсуждением будущих направлений в области криптографии для БПЛА.

Тема 4. **Безопасность сетевых соединений БПЛА**

В этой лекции рассматриваются аспекты безопасности сетевых соединений, используемых БПЛА. Студенты узнают о различных протоколах связи, таких как Wi-Fi, LTE и другие. Обсуждаются угрозы, связанные с беспроводными соединениями, включая перехват и вмешательство. Лекция включает анализ методов защиты сетевых соединений, таких как VPN и WPA3. Также рассматриваются вопросы аутентификации и авторизации пользователей. Студенты познакомятся с методами мониторинга сетевого трафика и обнаружения вторжений. Важным аспектом является необходимость обеспечения безопасности на всех уровнях сети. Лекция завершится обсуждением будущих тенденций в области сетевой безопасности для БПЛА.

Тема 5. **Управление инцидентами кибербезопасности БПЛА**

В этой лекции рассматриваются процессы управления инцидентами кибербезопасности, специфичные для БПЛА. Студенты узнают о методах обнаружения и реагирования на инциденты. Обсуждаются этапы управления инцидентами, включая подготовку, обнаружение, анализ, реагирование и восстановление. Лекция включает примеры успешного управления инцидентами в области БПЛА. Также рассматриваются вопросы документирования и анализа инцидентов для предотвращения повторения. Студенты познакомятся с инструментами и методами для мониторинга и анализа безопасности. Важным аспектом является необходимость обучения персонала в области управления инцидентами. Лекция завершится обсуждением лучших практик в управлении инцидентами кибербезопасности.

Тема 6. **Правовые и этические аспекты кибербезопасности БПЛА**

В этой лекции рассматриваются правовые и этические вопросы, связанные с кибербезопасностью БПЛА. Студенты узнают о законодательных актах и нормативных требованиях, регулирующих использование БПЛА. Обсуждаются вопросы конфиденциальности данных и защиты личной информации. Лекция включает анализ этических дилемм, связанных с использованием БПЛА в различных сферах. Также рассматриваются вопросы ответственности за кибератаки и инциденты безопасности. Студенты познакомятся с международными стандартами и соглашениями в области кибербезопасности. Важным аспектом является необходимость соблюдения правовых норм на всех уровнях. Лекция завершится обсуждением будущих тенденций в правовом регулировании кибербезопасности БПЛА.

Тема 7. **Аудит и оценка кибербезопасности БПЛА**

В этой лекции рассматриваются методы аудита и оценки кибербезопасности БПЛА. Студенты узнают о различных подходах к проведению аудита, включая внутренние и внешние проверки. Обсуждаются стандарты и методологии, используемые для оценки безопасности систем БПЛА. Лекция включает примеры успешных аудитов и их результатов. Также рассматриваются вопросы документирования и отчетности по результатам аудита. Студенты познакомятся с инструментами и методами для проведения оценки рисков. Важным аспектом является необходимость регулярного аудита для поддержания уровня безопасности. Лекция завершится обсуждением лучших практик в области аудита кибербезопасности.

Тема 8. **Технологии защиты БПЛА от кибератак**

В этой лекции рассматриваются современные технологии и методы защиты БПЛА от кибератак. Студенты узнают о системах обнаружения вторжений, антивирусных решениях и фаерволах. Обсуждаются методы шифрования и аутентификации для защиты данных и связи. Лекция включает примеры успешного применения технологий защиты в реальных сценариях. Также рассматриваются вопросы интеграции технологий безопасности в существующие системы БПЛА. Студенты познакомятся с новыми разработками в области защиты БПЛА. Важным аспектом является необходимость постоянного обновления технологий защиты. Лекция завершится обсуждением будущих направлений в области технологий защиты БПЛА.

4.3 Лекции

№ п/п	Название темы	Объем часов	
		Очная форма	**Заочная форма**
1	Введение в кибербезопасность БПЛА	**4**	
2	Угрозы и уязвимости БПЛА	**4**	
3	Криптография и защита данных в БПЛА	**4**	
4	Безопасность сетевых соединений БПЛА	**4**	
5	Управление инцидентами кибербезопасности БПЛА	**4**	
6	Правовые и этические аспекты кибербезопасности БПЛА	**4**	
7	Аудит и оценка кибербезопасности БПЛА	**5**	

8	Технологии защиты БПЛА от кибератак	**5**	
Итого:		**34**	

4.4 Практические (семинарские) занятия

№ п/п	Название темы	Объем часов	
		Очная форма	**Заочная форма**
1	Введение в кибербезопасность БПЛА	**2**	
2	Угрозы и уязвимости БПЛА	**2**	
3	Криптография и защита данных в БПЛА	**2**	
4	Безопасность сетевых соединений БПЛА	**2**	
5	Управление инцидентами кибербезопасности БПЛА	**2**	
6	Правовые и этические аспекты кибербезопасности БПЛА	**2**	
7	Аудит и оценка кибербезопасности БПЛА	**2**	
8	Технологии защиты БПЛА от кибератак	**3**	
Итого:		**17**	

4.5 Лабораторные работы

Не предусмотрено планом

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов	
			Очная форма	**Заочная форма**
1	Введение в кибербезопасность БПЛА	Подготовка к практическому занятию и к промежуточной аттестации.	7	
2	Угрозы и уязвимости БПЛА	Подготовка к практическому занятию и к промежуточной аттестации.	7	
3	Криптография и защита данных в БПЛА	Подготовка к практическим занятиям и к промежуточному контролю. Самостоятельный поиск источников информации.	7	
4	Безопасность сетевых соединений БПЛА	Подготовка к практическим занятиям и к промежуточному контролю. Самостоятельный поиск источников информации.	7	
5	Управление инцидентами кибербезопасности БПЛА	Подготовка к практическим занятиям, самостоятельный поиск источников информации.	7	

6	Правовые и этические аспекты кибербезопасности БПЛА	Подготовка к практическим занятиям, самостоятельный поиск источников информации.	7	
7	Аудит и оценка кибербезопасности БПЛА	Подготовка к практическим занятиям, самостоятельный поиск источников информации.	7	
8	Технологии защиты БПЛА от кибератак	Подготовка к практическим занятиям, самостоятельный поиск источников информации.	8	
Итого:			**57**	

4.7 Курсовые работы/проекты по дисциплине «Кибербезопасность БАС»

Курсовые работы не предусмотрены планом.

5 Образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий: объяснительно-иллюстративного обучения (технология поддерживающего обучения, технология проведения учебной дискуссии), информационных технологий (презентационные материалы), развивающих и инновационных образовательных технологий.

Практические занятия проводятся с использованием развивающих, проблемных, проектных, информационных (использование электронных образовательных ресурсов (электронный конспект) образовательных технологий и беспилотных летательных аппаратов.

6 Учебно-методическое и программно-информационное обеспечение дисциплины

а) основная литература:

1. Матвеев С.С., Донец С.И. **«Безопасность полётов в гражданской авиации».** Методическое указание по изучению курса и выполнению контрольной работы., С.С. Матвеев, С.И. Донец, Университет ГА, С.-Петербург, 2014 - 93с. Количество экземпляров – 500.

2. Никулин Н.Ф., Волков Г.А. **Управление безопасностью полётов в гражданской авиации. «Обеспечение безопасности полётов». Часть 1.** Учебно-методическое пособие. Н.Ф.Никулин, Г.А.Волков [Текст лекций], Университет ГА, С.-Петербург, 2015 - 104с. Количество экземпляров – 300.

3. Никулин, Н.Ф., Волков Г.А. **Управление безопасностью полётов в гражданской авиации. «Система управления безопасностью полётов». Часть II.** Учебно-методическое пособие. Н.Ф.Никулин, Г.А.Волков [Текст лекций], Университет ГА, С.-Петербург, 2015 - 96с. Количество экземпляров –300.

4. ИКАО, **Приложение ИКАО №19 «Управление безопасностью полётов»** 2013 г., ISBN 978-92-9249-239-7 Режим доступа: http://aviadocs.net/icaodocs/Annexes/an19_cons_ru.pdf, свободный.

5. ИКАО, **Руководство по управлению безопасностью полётов (РУБП)** DOC 9859 AN/474, 2013 г., ISBN 978-92-9249-334-9 Режим доступа: http://uralfavt.ru/usr/2015-02-18%20Doc%209859%20Rukovod%20po%20SUBP% 20IKAO%202013.pdf, свободный.

6. Малкин В.Ю. Аэронавигация беспилотных летательных аппаратов. Курс «Введение в специальность»: учебное пособие /В.Ю. Малкин, Т.В. Победа, Г.В. Сыровой, С.Р. Комраз.- Луганск: ИП Орехов Д.А., 2024.-172 с. - ISBN 978-5-6052742-8-5

б) дополнительная литература:

1. Бачило И.Л. Информационное право [Электронный ресурс]: учебник / И. Л. Бачило. — 5-е изд., пер. и доп. — М.: Юрайт, 2019. — 419 с. — Режим доступа: https://urait.ru/bcode/431119

2. Баранова Е. К. Информационная безопасность и защита информации [Электронный ресурс]: учеб. пособие / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — Москва: РИОР: ИНФРА-М, 2017. — 322 с. — ISBN 978-5-16-103249-7. – Режим доступа: https://znanium.com/catalog/document?id=75646.

3. Гродзенский Я. С. Информационная безопасность [Электронный ресурс]: учебное пособие. – Москва: РГ-Пресс, 2020. – 144 с. - ISBN 978-5-9988-0845-6. – Режим доступа: http://ebs.prospekt.org/book/43070.

4. Рассолов И. М. Информационное право [Электронный ресурс]: учебник и практикум для вузов / И. М. Рассолов. — 5-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2020. — 347 с. — ISBN 978-5-534-04348-8. – Режим доступа: https://urait.ru/bcode/449839.

в) методические указания:

1. Методические указания по изучению бакалаврами дисциплины «Основы применения БАС» по направлению подготовки 25.03.03 «Аэронавигация», 20.03.01 «Техносферная безопасность», 20.05.01 «Пожарная безопасность» / Сост.: Сыровой Г.В., Атрошенко Д.В. – Луганск: Изд-во ЛГУ им. Владимира Даля, 2024 г. – 58 с.

2. Методические указания по изучению бакалаврами дисциплины «Введение в деятельность аэронавигации» по направлению подготовки 25.03.03 «Аэронавигация» профиля «Эксплуатация беспилотных авиационных систем» / Сост.: Сыровой Г.В., Атрошенко Д.В. – Луганск: Изд-во ЛГУ им. Владимира Даля, 2024 г. – 40 с.

г) интернет-ресурсы:

1. Министерство образования и науки Российской Федерации – http://минобрнауки.рф/
2. Федеральная служба по надзору в сфере образования и науки – http://obrnadzor.gov.ru/
3. Министерство образования и науки Луганской Народной Республики – https://minobr.su
4. Народный совет Луганской Народной Республики – https://nslnr.su
5. Портал Федеральных государственных образовательных стандартов высшего образования – http://fgosvo.ru
6. Федеральный портал «Российское образование» – http://www.edu.ru/
7. Информационная система «Единое окно доступа к образовательным ресурсам» – http://window.edu.ru/
8. Федеральный центр информационно-образовательных ресурсов – http://fcior.edu.ru/

Электронные библиотечные системы и ресурсы:

1. Электронно-библиотечная система «Консультант студента» – http://www.studentlibrary.ru/cgi-bin/mb4x
2. Электронно-библиотечная система «StudMed.ru» –https://www.studmed.ru

Информационный ресурс библиотеки образовательной организации:

1. Научная библиотека имени А. Н. Коняева – http://biblio.dahluniver.ru/

Информационные ресурсы:

1. Предметно-ориентированный Web-портал «CALS-CAD-CAM-CAE-технологии» [Электронный ресурс]. – Режим доступа: http://cad.tu-bryansk.ru. – Загл. С экрана – Яз. рус.
2. **Единое окно доступа к образовательным ресурсам** [Электронный ресурс]. – Режим доступа: http://window.edu.ru/.

7 Материально-техническое обеспечение дисциплины

Освоение дисциплины «Кибербезопасность БАС» предполагает использование академических аудиторий, соответствующих действующим санитарным и противопожарным правилам и нормам.

Прочее: рабочее место преподавателя, оснащенное компьютером с доступом в Интернет, беспилотные летательные аппараты, спортивная площадка.

Программное обеспечение:

Функциональное назначение	**Бесплатное программное обеспечение**	**Ссылки**
Офисный пакет	Libre Office 6.3.1	https://www.libreoffice.org/ https://ru.wikipedia.org/wiki/LibreOffice
Операционная система	UBUNTU 19.04	https://ubuntu.com/ https://ru.wikipedia.org/wiki/Ubuntu
Браузер	Firefox Mozilla	http://www.mozilla.org/ru/firefox/fx
Браузер	Opera	http://www.opera.com
Почтовый клиент	Mozilla Thunderbird	http://www.mozilla.org/ru/thunderbird
Файл-менеджер	Far Manager	http://www.farmanager.com/download.php
Архиватор	7Zip	http://www.7-zip.org/
Графический редактор	GIMP (GNU Image Manipulation Program)	http://www.gimp.org/ http://gimp.ru/viewpage.php?page_id=8 http://ru.wikipedia.org/wiki/GIMP
Редактор PDF	PDFCreator	http://www.pdfforge.org/pdfcreator
Аудиоплейер	VLC	http://www.videolan.org/vlc/

8. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации по дисциплине (модулю)

Паспорт
оценочных средств по учебной дисциплине
«Кибербезопасность БАС»
Описание уровней сформированности и критериев оценивания компетенций на этапах их формирования в ходе изучения дисциплины

Этап	Код компетенции	Уровни сформирован-ности компетенции	Критерии оценивания компетенции
Начальный	ПК-11. Способен проводить мероприятия по обеспечению безопасности на ВТ	**Пороговый**	**знать:** - показатели кибербезопасности полетов воздушных судов; - факторы, влияющие на кибербезопасность полётов; -терминологию, основные определения и формулировки, используемые при характеристике состояния кибербезопасности полетов;
Основной		**Базовый**	**уметь:** -выполнять мероприятия, направленные на обеспечения кибербезопасности полетов воздушных судов, кибербезопасности использования воздушного пространства; -применять законодательство и нормативно правовые акты Российской Федерации, в области кибербезопасности полетов в профессиональной деятельности;
Заключительный		**Высокий**	**владеть:** методами и процедурами обеспечения кибербезопасности полетов воздушных судов и использования воздушного пространства; навыками применения законодательства и нормативных правовых актов Российской Федерации, международных стандартов и рекомендуемой практики в целях обеспечения кибербезопасности полётов воздушных судов и использования воздушного пространства.

Перечень компетенций (элементов компетенций), формируемых в результате освоения учебной дисциплины

№ п/п	Код компетенции	Формулировка контролируемой компетенции	Индикаторы достижений компетенции (по дисциплине)	Темы учебной дисциплины	Этапы формирования (семестр изучения)
1.	ПК-11	Способен проводить мероприятия по обеспечению безопасности на ВТ	ПК-11.1 принимает решение по управлению БВС СВТ с использованием знаний в области человеческого фактора; ПК-11.2 обнаруживает и реагирует на аварийные и необычные ситуации, связанные с операциями БВС, управлением в условиях ограниченной функциональности БВС и потери линии связи; ПК-11.3 участвует в проведении поисковых работ в случае аварийной посадки БВС СВТ.	*Тема 1. Введение в кибербезопасность БПЛА* *Тема 2. Угрозы и уязвимости БПЛА* *Тема 3. Криптография и защита данных в БПЛА* *Тема 4. Безопасность сетевых соединений БПЛА* *Тема 5. Управление инцидентами кибербезопасности БПЛА* *Тема 6. Правовые и этические аспекты кибербезопасности БПЛА* *Тема 7. Аудит и оценка кибербезопасности БПЛА* *Тема 8. Технологии защиты БПЛА от кибератак*	Начальный, Основной, Заключительный 4

Показатели и критерии оценивания компетенций, описание шкал оценивания

№ п/п	Код компетенции	Индикаторы достижений компетенции	Планируемые результаты обучения по дисциплине	Контролируемые темы учебной дисциплины	Наименование оценочного средства
1	ПК-11	ПК-11.1 принимает решение по управлению БВС СВТ с использованием	знать: - показатели кибербезопасности полетов воздушных судов; - факторы, влияющие на	*Тема 1. Введение в кибербезопасность БПЛА* *Тема 2. Угрозы и уязвимости БПЛА*	Вопросы для комбинированного контроля усвоения

		знаний в области человеческого фактора; ПК-11.2 обнаруживает и реагирует на аварийные и необычные ситуации, связанные с операциями БВС, управлением в условиях ограниченной функциональности БВС и потери линии связи; ПК-11.3 участвует в проведении поисковых работ в случае аварийной посадки БВС СВТ.	безопасность полётов; -терминологию, основные определения и формулировки, используемые при характеристике состояния безопасности полетов; уметь: -выполнять мероприятия, направленные на обеспечения кибербезопасности полетов воздушных судов, безопасности использования воздушного пространства; -применять законодательство и нормативно правовые акты Российской Федерации, в области кибербезопасности полетов в профессиональной деятельности; владеть: методами и процедурами обеспечения безопасности полетов воздушных судов и использования воздушного пространства; навыками применения законодательства и нормативных правовых актов Российской Федерации, международных	*Тема 3. Криптография и защита данных в БПЛА* *Тема 4. Безопасность сетевых соединений БПЛА* *Тема 5. Управление инцидентами кибербезопасности БПЛА* *Тема 6. Правовые и этические аспекты кибербезопасности БПЛА* *Тема 7. Аудит и оценка кибербезопасности БПЛА* *Тема 8. Технологии защиты БПЛА от кибератак*	теоретического материала, задания по практическим занятиям, реферат, зачет

			стандартов и рекомендуемой практики в целях обеспечения кибербезопасности полётов воздушных судов и использования воздушного пространства.		

1. Вопросы для комбинированного контроля усвоения теоретического материала (пороговый уровень):

1. Что такое БПЛА и какие основные функции они выполняют?
2. Каковы основные угрозы кибербезопасности, с которыми сталкиваются БПЛА?
3. Какие типы атак могут быть направлены на системы управления БПЛА?
4. Каковы основные уязвимости программного обеспечения БПЛА?
5. Как криптография может быть использована для защиты данных БПЛА?
6. Каковы методы аутентификации, применяемые в системах БПЛА?
7. Как осуществляется защита беспроводных соединений БПЛА от перехвата?
8. Каковы основные принципы управления инцидентами кибербезопасности для БПЛА?
9. Каковы правовые и этические аспекты кибербезопасности БПЛА?
10. Как осуществляется аудит и оценка кибербезопасности БПЛА?
11. Каковы лучшие практики для повышения осведомленности о кибербезопасности среди операторов БПЛА?
12. Как технологии искусственного интеллекта могут быть использованы для улучшения кибербезопасности БПЛА?
13. Каковы последствия успешной кибератаки на БПЛА?
14. Как осуществляется мониторинг и анализ сетевого трафика БПЛА для выявления угроз?
15. Каковы методы защиты БПЛА от атак "человек посередине"?
16. Каковы основные стандарты и нормативные акты, регулирующие кибербезопасность БПЛА?
17. Как осуществляется управление рисками в области кибербезопасности БПЛА?
18. Каковы современные технологии защиты БПЛА от кибератак?
19. Как осуществляется взаимодействие между различными организациями для обеспечения кибербезопасности БПЛА?
20. Каковы будущие тенденции в области кибербезопасности БПЛА и какие вызовы могут возникнуть?

Критерии и шкала оценивания по оценочному средству
«комбинированный контроль усвоения теоретического материала»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Ответ дан на высоком уровне (студент в полном объеме осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, владеет профильным понятийным (категориальным) аппаратом и т.п.)
4	Ответ дан на среднем уровне (студент в целом осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, допустив некоторые неточности и т.п.)

3	Ответ дан на низком уровне (студент допустил существенные неточности, изложил материал с ошибками, не владеет в достаточной степени профильным категориальным аппаратом и т.п.)
2	Ответ дан на неудовлетворительном уровне или не представлен (студент не готов, не выполнил задание и т.п.)

2. Тестовые задания

(пороговый уровень)

1. Какой из следующих типов атак наиболее распространен для БПЛА?
   A) DDoS-атака
   B) Физическое вмешательство
   C) Атака "человек посередине"
   D) Вирусная атака
   Ответ: C) Атака "человек посередине"

2. Какой метод шифрования чаще всего используется для защиты данных БПЛА?
   A) Симметричное шифрование
   B) Ассиметричное шифрование
   C) Хеширование
   D) Все вышеперечисленные
   Ответ: D) Все вышеперечисленные

3. Какой из следующих протоколов используется для безопасной передачи данных?
   A) HTTP
   B) FTP
   C) HTTPS
   D) SMTP
   Ответ: C) HTTPS

4. Какой из следующих аспектов не является частью управления инцидентами кибербезопасности?
   A) Обнаружение инцидента
   B) Реагирование на инцидент
   C) Устранение инцидента
   D) Разработка нового БПЛА
   Ответ: D) Разработка нового БПЛА

5. Какой из следующих методов может быть использован для аутентификации пользователей БПЛА?
   A) Пароль
   B) Биометрия
   C) Смарт-карты
   D) Все вышеперечисленные
   Ответ: D) Все вышеперечисленные

6. Какой из следующих стандартов регулирует кибербезопасность в авиации?
   A) ISO 9001
   B) ISO/IEC 27001

C) DO-326A
D) IEEE 802.11
Ответ: C) DO-326A

7. Какой из следующих методов защиты беспроводных соединений наиболее эффективен?
A) WEP
B) WPA
C) WPA2
D) Все вышеперечисленные
Ответ: C) WPA2

8. Какой из следующих инструментов используется для мониторинга сетевого трафика?
A) IDS (Intrusion Detection System)
B) VPN
C) Firewall
D) Все вышеперечисленные
Ответ: A) IDS (Intrusion Detection System)

9. Какой из следующих аспектов является важным для повышения осведомленности о кибербезопасности?
A) Регулярные тренинги
B) Документация
C) Политики безопасности
D) Все вышеперечисленные
Ответ: D) Все вышеперечисленные

10. Какой из следующих типов уязвимостей может быть использован для атаки на БПЛА?
A) Уязвимости программного обеспечения
B) Уязвимости аппаратного обеспечения
C) Уязвимости сети
D) Все вышеперечисленные
Ответ: D) Все вышеперечисленные

11. Какой из следующих методов может быть использован для защиты от атак "человек посередине"?
A) Шифрование данных
B) Использование VPN
C) Аутентификация
D) Все вышеперечисленные
Ответ: D) Все вышеперечисленные

12. Какой из следующих аспектов не является частью оценки рисков в кибербезопасности?
A) Идентификация угроз
B) Оценка уязвимостей
C) Разработка новых технологий
D) Анализ последствий
Ответ: C) Разработка новых технологий

13. Какой из следующих типов данных наиболее уязвим для кибератак?
A) Личные данные
B) Финансовые данные
C) Данные о полетах
D) Все вышеперечисленные
Ответ: D) Все вышеперечисленные

14. Какой из следующих методов может быть использован для защиты данных на БПЛА?
A) Шифрование
B) Резервное копирование
C) Контроль доступа
D) Все вышеперечисленные
Ответ: D) Все вышеперечисленные

15. Какой из следующих аспектов важен для обеспечения безопасности БПЛА?
A) Обновление программного обеспечения
B) Физическая безопасность
C) Обучение персонала
D) Все вышеперечисленные
Ответ: D) Все вышеперечисленные

16. Какой из следующих типов атак может привести к потере управления БПЛА?
A) DDoS-атака
B) Атака на систему навигации
C) Атака на систему связи
D) Все вышеперечисленные
Ответ: D) Все вышеперечисленные

17. Какой из следующих аспектов не является частью политики безопасности БПЛА?
A) Определение ролей и обязанностей
B) Процедуры реагирования на инциденты
C) Разработка новых БПЛА
D) Обучение сотрудников
Ответ: C) Разработка новых БПЛА

18. Какой из следующих инструментов может быть использован для защиты от вирусов?
A) Антивирусное ПО
B) Фаервол
C) IDS
D) Все вышеперечисленные
Ответ: A) Антивирусное ПО

19. Какой из следующих аспектов важен для обеспечения конфиденциальности данных БПЛА?
A) Шифрование
B) Аутентификация
C) Контроль доступа
D) Все вышеперечисленные

Ответ: D) Все вышеперечисленные

20. Какой из следующих методов может быть использован для защиты от утечек данных?
A) Шифрование
B) Мониторинг трафика
C) Политики безопасности
D) Все вышеперечисленные
Ответ: D) Все вышеперечисленные

Критерии и шкала оценивания по оценочному средству «тестирование»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	85 – 100% правильных ответов
4	71 – 85% правильных ответов
3	61 – 70% правильных ответов
2	60% правильных ответов и ниже

3. Практическое задание

(высокий уровень)

1. Задание: Провести анализ угроз для конкретного типа БПЛА (например, дрон для сельского хозяйства).

Ответ: Определить потенциальные угрозы, такие как перехват управления, вмешательство в навигацию, кража данных и физическое повреждение.

2. Задание: Разработать политику безопасности для оператора БПЛА.

Ответ: Включить разделы о доступе к данным, шифровании, аутентификации пользователей и реагировании на инциденты.

3. Задание: Провести тестирование на проникновение для системы управления БПЛА.

Ответ: Использовать инструменты, такие как Metasploit или Wireshark, для выявления уязвимостей и документирования результатов.

4. Задание: Создать план реагирования на инциденты для БПЛА.

Ответ: Определить этапы: обнаружение, анализ, реагирование, восстановление и отчетность.

5. Задание: Оценить риски кибербезопасности для БПЛА, используемого в логистике.

Ответ: Провести SWOT-анализ, выявить уязвимости и угрозы, оценить последствия и вероятность.

6. Задание: Разработать программу обучения по кибербезопасности для операторов БПЛА.

Ответ: Включить темы о распознавании угроз, безопасной эксплуатации и реагировании на инциденты.

7. Задание: Провести аудит безопасности программного обеспечения БПЛА.

Ответ: Проверить наличие обновлений, уязвимостей и соответствие стандартам безопасности.

8. Задание: Исследовать и представить методы шифрования данных, используемых в БПЛА.

Ответ: Рассмотреть симметричное и асимметричное шифрование, а также протоколы, такие как AES и RSA.

9. Задание: Разработать стратегию защиты беспроводных соединений БПЛА.

Ответ: Включить использование WPA3, VPN и регулярный мониторинг сетевого трафика.

10. Задание: Создать отчет о последствиях кибератаки на БПЛА.

Ответ: Описать возможные последствия, такие как потеря данных, повреждение оборудования и репутационные риски.

11. Задание: Провести анализ уязвимостей для системы управления полетом БПЛА.

Ответ: Использовать инструменты, такие как Nessus, для выявления уязвимостей и предложить меры по их устранению.

12. Задание: Разработать план резервного копирования данных для БПЛА.

Ответ: Определить частоту резервного копирования, методы хранения и восстановление данных.

13. Задание: Исследовать и представить примеры успешных кибератак на БПЛА.

Ответ: Описать инциденты, такие как атаки на дроны военных или коммерческих операторов, и их последствия.

14. Задание: Создать модель угроз для системы связи БПЛА.

Ответ: Определить возможные угрозы, такие как перехват, вмешательство и атаки на инфраструктуру связи.

15. Задание: Разработать рекомендации по физической безопасности для хранения БПЛА.

Ответ: Включить меры, такие как контроль доступа, видеонаблюдение и охрана.

16. Задание: Провести исследование о правовых аспектах кибербезопасности БПЛА.

Ответ: Изучить законы и нормативные акты, регулирующие использование БПЛА и защиту данных.

17. Задание: Разработать стратегию управления инцидентами для БПЛА.

Ответ: Определить роли и обязанности команды, а также процедуры для каждого этапа реагирования.

18. Задание: Оценить влияние новых технологий (например, ИИ) на кибербезопасность БПЛА.

Ответ: Рассмотреть как положительные, так и отрицательные аспекты, включая улучшение защиты и новые уязвимости.

19. Задание: Создать план тестирования на проникновение для системы управления БПЛА.

Ответ: Определить цели тестирования, методы и инструменты, а также процесс документирования результатов.

20. Задание: Разработать рекомендации по повышению осведомленности о кибербезопасности среди пользователей БПЛА.

Ответ: Включить регулярные тренинги, информационные бюллетени и создание культуры безопасности.

Критерии и шкала оценивания по оценочному средству *«практическое задание»*

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Практические задания выполнены на высоком уровне (правильные ответы даны на 90 – 100% вопросов/задач)
4	Практические задания выполнены на среднем уровне (правильные ответы даны на 75 – 89% вопросов/задач)
3	Практические задания выполнены на низком уровне (правильные ответы даны на 50 – 74% вопросов/задач)
2	Практические задания выполнены на неудовлетворительном уровне (правильные ответы даны менее чем на 50%)

4. Реферат

(базовый уровень)

1. Анализ угроз кибербезопасности для БПЛА

Исследование основных угроз, с которыми сталкиваются беспилотные летательные аппараты, и их потенциальные последствия.

2. Методы защиты данных в системах БПЛА

Обзор технологий шифрования и других методов защиты данных, используемых в БПЛА.

3. Криптография в кибербезопасности БПЛА

Роль криптографических методов в обеспечении безопасности передачи данных и управления БПЛА.

4. Атаки на системы управления БПЛА

Анализ различных типов атак, направленных на системы управления беспилотниками, и способы их предотвращения.

5. Правовые аспекты кибербезопасности БПЛА

Обзор законодательства и нормативных актов, регулирующих использование БПЛА и защиту данных.

6. Управление инцидентами кибербезопасности для БПЛА

Процессы и процедуры, необходимые для эффективного реагирования на инциденты кибербезопасности.

7. Физическая безопасность БПЛА

Меры по обеспечению физической безопасности беспилотных летательных аппаратов и их компонентов.

8. Роль искусственного интеллекта в кибербезопасности БПЛА

Как технологии ИИ могут быть использованы для улучшения безопасности БПЛА.

9. Аудит и оценка кибербезопасности БПЛА

Методы и подходы к проведению аудита безопасности систем БПЛА.

10. Обучение и повышение осведомленности о кибербезопасности для операторов БПЛА

Программы и методы обучения, направленные на повышение уровня осведомленности о киберугрозах.

11. Технологии защиты беспроводных соединений БПЛА

Обзор методов и протоколов, используемых для защиты беспроводных соединений.

12. Кейс-стадии кибератак на БПЛА

Анализ реальных случаев кибератак на беспилотные летательные аппараты и их последствия.

13. Уязвимости программного обеспечения БПЛА

Исследование распространенных уязвимостей в программном обеспечении БПЛА и способы их устранения.

14. Этические аспекты кибербезопасности БПЛА

Обсуждение этических вопросов, связанных с использованием БПЛА и кибербезопасностью.

15. Будущее кибербезопасности БПЛА: вызовы и возможности

Прогнозирование будущих тенденций в области кибербезопасности для беспилотников.

16. Интеграция кибербезопасности в жизненный цикл БПЛА

Как кибербезопасность должна быть встроена на всех этапах разработки и эксплуатации БПЛА.

17. Методы тестирования на проникновение для БПЛА

Обзор подходов и инструментов, используемых для тестирования безопасности БПЛА.

18. Роль стандартов и нормативов в кибербезопасности БПЛА

Как международные и национальные стандарты влияют на безопасность БПЛА.

19. Системы обнаружения вторжений для БПЛА

Обзор технологий и методов, используемых для обнаружения и предотвращения кибератак.

20. Кибербезопасность БПЛА в военных и гражданских приложениях

Сравнительный анализ требований к кибербезопасности в военных и гражданских БПЛА.

Критерии и шкала оценивания по оценочному средству» реферат»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Реферат представлен на высоком уровне (студент в полном объеме осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, владеет профильным понятийным (категориальным) аппаратом и т.п.). Оформлен в соответствии с требованиями, предъявляемыми к данному виду работ
4	Реферат представлен на среднем уровне (студент в целом осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, допустив некоторые неточности и т.п.). В оформлении допущены некоторые неточности в соответствии с требованиями, предъявляемыми к данному виду работ
3	Реферат представлен на низком уровне (студент допустил существенные неточности, изложил материал с ошибками, не владеет в достаточной степени профильным категориальным аппаратом и т.п.). В оформлении допущены ошибки в соответствии с требованиями, предъявляемыми к данному виду работ
2	Реферат представлен на неудовлетворительном уровне или не представлен (студент не готов, не выполнил задание и т.п.)

5. Оценочные средства по зачету

Вопросы к зачету

1. Что такое БПЛА и какие основные функции они выполняют?
2. Какие типы угроз кибербезопасности наиболее актуальны для БПЛА?
3. Каковы основные уязвимости программного обеспечения БПЛА?
4. Что такое атака "человек посередине" и как она может повлиять на БПЛА?
5. Каковы последствия успешной кибератаки на БПЛА?
6. Какие методы шифрования используются для защиты данных БПЛА?
7. Как осуществляется аутентификация пользователей в системах БПЛА?

8. Какие протоколы безопасности применяются для защиты беспроводных соединений БПЛА?

9. Каковы основные этапы анализа рисков для БПЛА?

10. Как осуществляется мониторинг и анализ сетевого трафика БПЛА?

11. Какие меры можно предпринять для защиты БПЛА от DDoS-атак?

12. Каковы правовые аспекты кибербезопасности БПЛА?

13. Как осуществляется управление инцидентами кибербезопасности для БПЛА?

14. Какие технологии используются для обнаружения вторжений в системы БПЛА?

15. Каковы основные принципы разработки политики безопасности для БПЛА?

16. Какова роль обучения и повышения осведомленности в кибербезопасности БПЛА?

17. Какие примеры реальных кибератак на БПЛА известны?

18. Каковы методы тестирования на проникновение для систем БПЛА?

19. Как осуществляется оценка уязвимостей в системах БПЛА?

20. Каковы основные стандарты и нормативные акты, регулирующие кибербезопасность БПЛА?

21. Каковы последствия утечки данных, связанных с БПЛА?

22. Как технологии искусственного интеллекта могут быть использованы для повышения безопасности БПЛА?

23. Каковы основные аспекты физической безопасности БПЛА?

24. Как осуществляется защита от атак на систему навигации БПЛА?

25. Каковы методы защиты данных, передаваемых между БПЛА и наземными станциями?

26. Каковы вызовы и возможности для кибербезопасности БПЛА в будущем?

27. Как осуществляется интеграция кибербезопасности в жизненный цикл БПЛА?

28. Каковы основные угрозы, связанные с использованием БПЛА в коммерческих целях?

29. Каковы методы управления рисками в кибербезопасности БПЛА?

30. Каковы лучшие практики для обеспечения кибербезопасности БПЛА?

Критерии и шкала оценивания по оценочному средству – зачет.

Шкала оценивания	Характеристика знания предмета и ответов
зачет	Студент глубоко и в полном объёме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопросы и правильно обосновывает принятые решения, хорошо владеет умениями и навыками при выполнении практических задач.
незачет	Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы

6. Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости рабочая программа учебной дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе с применением электронного обучения и дистанционных образовательных технологий.

Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК). В случае необходимости обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося), а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей:

– 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 (модулем), за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

– применение электронного обучения, 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 электронного обучения, 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:

– продолжительность сдачи зачёта или экзамена, проводимого в письменной форме, – не более чем на 90 минут;

– продолжительность подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, – не более чем на 20 минут;

– продолжительность выступления обучающегося при защите курсовой работы – не более чем на 15 минут.

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений с указанием страниц	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)
1.			
2.			
3.			
4.			