

Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Донецкий государственный университет»

Факультет физико-технический
Кафедра радиофизики и инфокоммуникационных технологий



УТВЕРЖДАЮ
проректор

П.А. Машаров

«29» марта 2024 г.

МП

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ЗАЩИТА СИСТЕМ УПРАВЛЕНИЯ БЕСПИЛОТНЫХ
ЛЕТАТЕЛЬНЫХ АППАРАТОВ»**

Укрупненная группа направлений подготовки	10.00.00 Информационная безопасность
Программа высшего образования	Программа магистратуры
Направление подготовки	10.04.01 Информационная безопасность
Магистерская программа	Информационная безопасность
Квалификация	Магистр
Форма обучения	очная; очно-заочная

Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины «Защита систем управления беспилотными летательными аппаратами» для обучающихся по направлению подготовки 10.04.01 Информационная безопасность (Магистерская программа: Информационная безопасность), составлена на основании Федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации Приказ от 26 ноября 2020 г. № 1455(с изм. и доп.). Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06 апреля 2021 г. № 245 (с изм. и доп.), в соответствии с учебным планом, утвержденным Ученым советом ФГБОУ ВО «ДонГУ» для набора 2024 года.

Разработчик:

Ст. преподаватель
кафедры радиофизики
и инфокоммуникационных технологий



Е.Н. Кожекина

Рабочая программа утверждена на заседании кафедры радиофизики и инфокоммуникационных технологий
Протокол от 26.03.2024 г. № 16

Заведующий кафедрой



В.В. Данилов

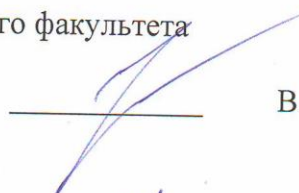
СОГЛАСОВАНО:

И.о. декана физико-технического факультета
28.03.2024 г.



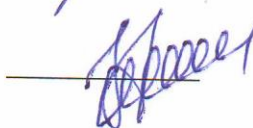
С.А. Фоменко

Учебно-методическая комиссия физико-технического факультета
Протокол от 27.03.2024 г. № 2
Председатель



В. Н. Котенко

Руководитель основной профессиональной образовательной программы
д-р тех. наук, проф.
26.03.2024 г.



В.В. Данилов

1. МЕСТО ДИСЦИПЛИНЫ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Требования к предварительной подготовке обучающихся, предшествующие и сопутствующие дисциплины, на которых основывается изучение данной:
 базовая подготовка по математике в объеме программы средней школы;
 дисциплины программы бакалавриата: Системы управления беспилотными летательными аппаратами, Основы управления информационной безопасностью, Построение защищенных микропроцессорных систем, Методы и средства криптографической защиты информации

1.2. Дисциплины, курсовые работы и практики, для которых освоение данной дисциплины необходимо как предшествующее:
 Технологии обеспечения информационной безопасности объектов,
 Производственная практика: научно-исследовательская работа (обязательная),
 Производственная практика: преддипломная практика (обязательная).

2. ОПИСАНИЕ ДИСЦИПЛИНЫ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	10.04.01 Информационная безопасность (Магистерская программа: Информационная безопасность)
Шифр и название в соответствии с учебным планом	Б1.В.ДВ.2.1 Защита беспилотных летательных аппаратов
Часть образовательной программы	Вариативная часть: выбор обучающегося
Количество зачетных единиц / всего часов	4 / 144

2.2. Распределение часов по формам и периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы + контроль	всего	
Очная, всего	1	2	15	30	15	84	144	экзамен
Очная-заочная, всего	3	5	4	10	4	126	144	экзамен

3. ЦЕЛИ ДИСЦИПЛИНЫ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Формирование у студентов теоретических знаний и практических навыков, необходимых для защиты систем управления беспилотных летательных аппаратов (БПЛА) от внешних и внутренних угроз. Дисциплина направлена на изучение принципов обеспечения безопасности, методов предотвращения и обнаружения атак, а также разработки и внедрения защитных мер для сохранения устойчивости и надежности систем управления БПЛА в различных условиях эксплуатации.

4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ КОМПОНЕНТА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, ИХ ИНДИКАТОРЫ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

4.1. Компетенции

Компетенции	Индикаторы	Результаты обучения
ПК-1. Способен разрабатывать программные, программно-аппаратные, программно-технические, технические средства и системы защиты информации	ПК-1.3 Разработка программно-аппаратных средств для систем защиты информации автоматизированных систем	ПК-1.3.1. Понимание основных угроз безопасности БПЛА, таких как перехват управления, глушение сигнала и взлом сети. ПК-1.3.2. Навыки практических методов шифрования данных, защищенной передачи команд и применения аутентификации для предотвращения несанкционированного доступа. ПК-1.3.3. Знание слабых мест в программном обеспечении, аппаратной структуре и коммуникационных каналах, что помогает в обнаружении и устранении потенциальных рисков.

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
1. Угрозы и уязвимости в системах управления БПЛА	Виды атак: физические, кибернетические, радиоэлектронные. Уязвимости программного обеспечения и аппаратных компонентов. Угрозы безопасности на разных этапах полета.
2. Основы криптографии и шифрования данных	Основы криптографии для защиты данных. Симметричные и асимметричные алгоритмы шифрования. Применение криптографии в системах управления БПЛА.
3. Аутентификация и контроль доступа	Методы аутентификации операторов и устройств. Протоколы и механизмы контроля доступа. Применение мультифакторной аутентификации в управлении БПЛА
4. Методы обнаружения атак и предотвращения угроз	Мониторинг и анализ сетевого трафика. Системы обнаружения вторжений (IDS) и предотвращения атак (IPS). Использование искусственного интеллекта для обнаружения угроз.
5. Защита радиоэлектронного канала управления	Особенности радиосвязи в системах управления БПЛА. Методы защиты радиоканалов от перехвата и глушения. Протоколы шифрования и защищенного обмена данными.
6. Методы обеспечения устойчивости систем управления	Методы резервирования и дублирования критических систем.

	Программные и аппаратные решения для повышения устойчивости. Применение технологий самовосстановления и реорганизации.
7. Планирование и тестирование безопасности	Методология оценки безопасности системы управления. Стандарты и требования безопасности для систем управления БПЛА. Проведение тестирования на проникновение и моделирование атак.
8. Управление инцидентами и реагирование на угрозы	Процессы и протоколы реагирования на инциденты. Документирование и анализ инцидентов. Пост-инцидентное восстановление и меры по предотвращению повторных атак.

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6.1. Форма обучения – очная, курс – 1, семестр – 2

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
1. Угрозы и уязвимости в системах управления БПЛА	1	4	2	10	17
2. Основы криптографии и шифрования данных	2	3	2	10	17
3. Аутентификация и контроль доступа	2	4	2	10	18
4. Методы обнаружения атак и предотвращение угроз	2	4	2	12	20
5. Защита радиоэлектронного канала управления	2	4	2	10	18
6. Методы обеспечения устойчивости систем управления	2	4	2	10	18
7. Планирование и тестирование безопасности	2	4	1	10	17
8. Управление инцидентами и реагирование на угрозы	2	3	2	12	19
ИТОГО ЗА СЕМЕСТР ПО КОМПОНЕНТУ ОПОП	15	30	15	84	144

6.2. Форма обучения – очно-заочная, курс – 3, семестр – 5

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
1 Угрозы и уязвимости в системах управления БПЛА	0.5	1	0.5	16	18
2 Основы криптографии и шифрования данных	0.5	1	0.5	16	18
3 Аутентификация и контроль доступа	0.5	1	0.5	15	17
4 Методы обнаружения атак и предотвращение угроз	0.5	1	0.5	16	18

5 Защита радиоэлектронного канала управления	0.5	2	0.5	15	19
6 Методы обеспечения устойчивости систем управления	0.5	2	0.5	16	20
7 Планирование и тестирование безопасности	0.5	1	0.5	16	18
8 Управление инцидентами и реагирование на угрозы	0.5	1	0.5	16	18
ИТОГО ЗА СЕМЕСТР ПО КОМПОНЕНТУ ОПОП	4	10	4	126	144

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Контрольные вопросы

1. Какие основные угрозы безопасности существуют для систем управления беспилотных летательных аппаратов (БПЛА)?
2. Что такое перехват управления БПЛА, и как его можно предотвратить?
3. Какой метод шифрования данных чаще всего используется в БПЛА для защиты информации?
4. Что представляет собой аутентификация, и почему она важна для защиты систем БПЛА?
5. Какие типы атак возможны на каналы связи между БПЛА и оператором?
6. Каковы основные способы защиты от глушения сигнала БПЛА?
7. В чем разница между пассивной и активной защитой систем управления БПЛА?
8. Какие уязвимости в аппаратном обеспечении БПЛА могут представлять угрозу для его безопасности?
9. Какие методы используются для мониторинга сетевого трафика БПЛА и обнаружения аномальной активности?
10. Какие угрозы возникают при использовании GPS для навигации БПЛА?
11. Что такое DDoS-атака, и каким образом она может быть направлена на системы управления БПЛА?
12. Какой вклад в защиту БПЛА вносит шифрование каналов связи?
13. Как построить эффективную систему обнаружения атак для БПЛА?
14. В чем заключается роль оператора при реагировании на инциденты в системах управления БПЛА?
15. Какие правовые и этические аспекты нужно учитывать при использовании и защите БПЛА?
16. Что такое "цифровая подпись", и как она помогает защищать данные БПЛА?
17. Какие меры необходимо предпринять для защиты данных, записанных на устройствах памяти БПЛА?
18. Какие технологии аутентификации считаются наиболее эффективными для защиты систем управления БПЛА?
19. Какие действия должен предпринять оператор в случае обнаружения перехвата управления?
20. Каковы основные принципы проектирования устойчивых к атакам беспилотных систем?

7.2. Темы докладов (рефератов)

1. Актуальные угрозы безопасности беспилотных летательных аппаратов и их систем управления

2. Методы защиты от перехвата управления БПЛА и несанкционированного доступа
3. Роль шифрования данных и защищенной передачи команд в безопасности БПЛА
4. Защита каналов связи от глушения и подмены сигналов: современные подходы
5. Обзор уязвимостей в архитектуре и программном обеспечении БПЛА
6. Применение систем аутентификации и авторизации для защиты БПЛА
7. Использование искусственного интеллекта для защиты БПЛА от кибератак
8. Методы мониторинга сетевого трафика БПЛА и обнаружения аномальной активности
9. Защита GPS-навигации БПЛА от спуфинга и глушения сигнала
10. Этические и правовые аспекты защиты и применения беспилотников
11. Роль оператора в обеспечении безопасности и реагировании на инциденты с БПЛА
12. Построение системы обнаружения и предотвращения атак на БПЛА
13. Принципы защиты данных на борту БПЛА и предотвращение их утечки
14. Атаки на беспилотные летательные аппараты: примеры и анализ инцидентов
15. Перспективы развития технологий для повышения безопасности БПЛА

7.3.Образец содержания экзаменационного билета

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Донецкий государственный университет

Физико-технический факультет

Кафедра радиофизики и инфокоммуникационных технологий

Программа высшего образования	Программа магистратура
Направление подготовки	10.04.01 Информационная безопасность
Профиль подготовки	Безопасность автоматизированных систем
Форма обучения	Очная
Семестр	Второй
Дисциплина	Защита систем управления беспилотных летательных аппаратов

Экзаменационный билет № 1

1. Опишите механизмы защиты от GPS-спуфинга в БПЛА. Какие недостатки имеются у текущих решений, и как их можно устранить в будущем?
2. Как работает система обнаружения атак на основе анализа аномалий в поведении БПЛА? Какие алгоритмы и методы используются для повышения точности таких систем, и как они адаптируются к новым типам угроз?
3. Проанализируйте возможные уязвимости в коммуникационных протоколах БПЛА. Как могут использоваться методы криптографической защиты для устранения данных уязвимостей, и какие ограничения это может наложить на производительность системы?

Утверждено на заседании кафедры радиофизики и инфокоммуникационных технологий,
протокол № __ от __. __.202__ г.

Заведующий кафедрой

В.В. Данилов

Экзаменатор

Е.Н. Кожекина

8. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Общая оценка знаний обучающихся по дисциплине проводится по 100-балльной шкале исходя из максимума, приведенного в таблице ниже. Организационно-учебная работа в аудитории оценивается на основе таких критериев как посещаемость занятий, своевременное и качественное выполнение домашних заданий, активность во время проведения лекционных и практических занятий (участие в обсуждении текущего и пройденного материала, решение задач и т.п.).

8.1. Семестр 1

Номера разделов	Виды работ	Максимальное количество баллов
1-8	Организационно-учебная работа в аудитории	6
	Лабораторные работы	17
	Практические работы	17
	Доклад по выбранной теме	10
ИТОГО		50
Экзамен		50
Общий итог за семестр		100

Соответствие баллов оценке

Количество баллов из 100	ECTS	Оценка по пятибалльной шкале	
		Экзамен, дифференцированный зачет	Зачет
90-100	A	отлично	зачтено
80-89	B	хорошо	зачтено
75-79	C		зачтено
70-74	D	удовлетворительно	зачтено
60-69	E		зачтено
35-59	FX	неудовлетворительно	не зачтено
0-34	F		не зачтено

9. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- 1) для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
 - письменные задания оформляются увеличенным шрифтом.
- 2) для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа;
 - письменные задания выполняются на компьютере в письменной форме;
 - экзамен проводится в письменной форме на компьютере; возможно проведение в форме тестирования.
- 3) для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- 1) для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
- 2) для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- 3) для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в Главном корпусе ДонГУ (г. Донецк, пр. Гурова, 6). Для проведения лекционных и практических занятий требуется аудитория, оборудованная меловой или маркерной доской, мультимедийный проектор и экран, ноутбук, комплект учебной мебели для студентов, рабочее место преподавателя, выход в Интернет – проводной или с использованием Wi-Fi.

Для проведения лабораторных занятий требуется лаборатория, обеспеченная персональными компьютерами, макеты БПЛА с возможностью программирования.

Для самостоятельной работы используются текстовые и электронные ресурсы Научной библиотеки университета и других электронных библиотечных баз данных, учебно-методическое обеспечение, представленное в учебно-методическом кабинете Главного корпуса (ауд.405).

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные на платформе Moodle Центра дистанционного образования ФГБОУ ВО «ДонГУ». При изучении дисциплины применяются электронное обучение и дистанционные образовательные технологии.

С использованием ресурсов платформы дистанционного образования осуществляется текущий контроль знаний обучающихся на основе тестирования и проверки результатов самостоятельной работы.

11. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

11.1. Основная литература

1. Корт, С. С. Теоретические основы защиты информации : Учеб. пособие для студентов вузов, обучающихся по группе спец. в обл. информ. безопасности / С. С. Корт. - М. : Гелиос АРВ, 2004. - 233 с.

2. Кибербезопасность беспилотных авиационных систем. Беспилотная авиационная система как объект информационной защиты [Текст] : учебное пособие / Э.А. Болелов,, К.И. Галаева. – М. : ИД Академии Жуковского, 2023. – 80 с

11.2. Дополнительная литература

1. Информационная безопасность открытых систем [Текст] : учебник для студентов вузов, обучающихся по специальности 075500 (090105) - "Комплексное обеспечение информационной безопасности автоматизированных систем" : [в 2 т.]. Т. 1 : Угрозы, уязвимости, атаки и подходы к защите / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. - М. : Горячая Линия-Телеком, 2006. - 535 с.

2. Макаренко С. И. Противодействие беспилотным летательным аппаратам. Монография. – СПб.: Научные технологии, 2020. – 204 с.

12. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. **Национальная электронная библиотека (НЭБ):** федеральная государственная информационная система / Министерство Культуры РФ; Российская государственная библиотека. – Москва, 2019- . – URL: <https://rusneb.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный, подписка. Необходима установка программного обеспечения. – Текст: электронный.

2. **eLIBRARY.RU:** научная электронная библиотека: сайт. – Москва, 2000- . – URL: <https://elibrary.ru> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

3. Научная электронная библиотека **«КиберЛенинка»:** сайт / Ассоциация «Открытая наука». – Москва, 2014- . – URL: <https://cyberleninka.ru/>. – Режим доступа: свободный. – Текст: электронный.

4. Электронно-библиотечная система **«Лань»:** [сайт]. – URL: <https://e.lanbook.com> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

5. **ЭБС Юрайт:** электронная библиотечная система: сайт. – Москва, 2013. – URL: <https://biblio-online.ru> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

6. **Электронно-библиотечная система ДонГУ:** сайт / ФГБОУ ВО «ДонГУ». – Донецк, 2016- . – URL: <http://library.donnu.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный. – Текст: электронный.

7. **Электронный каталог** Научной библиотеки ДонГУ: раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://library.donnu.ru/catalog/> (дата обращения: 01.09.2023). – Режим доступа: поиск свободный, электронные документы – для пользователей ДонГУ.

8. **Электронный архив ДонГУ:** раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://repo.donnu.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный.

13. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонГУ № 46484614)
 2. Microsoft Office (корпоративная лицензия ДонГУ № 46472919)
 3. Microsoft Visual Studio (лицензия программы Dream Spark для высших учебных заведений)

4. Антивирус Касперского, Adobe Acrobat Reader, xPDF (лицензии GPL, Apache, BSD для свободного программного обеспечения).