ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА

(РОСАВИАЦИЯ)
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ ИМЕНИ ГЛАВНОГО МАРШАЛА АВИАЦИИ А.А. НОВИКОВА»

УТВЕРЖДАЮ

Ректор

_____ / Ю.Ю. Михальчевский

«23» ноября 2023 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Средства и методы защиты беспилотных авиационных систем

Направление подготовки
01.03.04 Прикладная математика

Направленность программы (профиль)
Математическое и программное обеспечение беспилотных авиационных систем

Квалификация выпускника
бакалавр

Форма обучения
очная

Санкт-Петербург
2023

1 Цели освоения дисциплины

Целью освоения дисциплины «Средства и методы защиты беспилотных авиационных систем» является формирование у студентов системы специальных знаний и прикладных навыков об основных принципах, алгоритмах, технических и организационных мерах по безопасному использованию беспилотных авиационных систем.

Задачами освоения дисциплины «Средства и методы защиты беспилотных авиационных систем» являются:

– формирование у обучающихся знаний об основных результатах в области криптографических исследований;

– приобретение обучающимися умений анализировать методы защиты линий передачи данных при решении задач защиты БАС;

– овладение обучающимися навыками моделирования процессов при решении задач защиты БАС.

Дисциплина обеспечивает подготовку выпускника к решению задач профессиональной деятельности научно-исследовательского типа.

2 Место дисциплины в структуре ОПОП ВО

Дисциплина «Средства и методы защиты беспилотных авиационных систем» представляет собой дисциплину, относящуюся к блоку «Факультативы».

Дисциплина «Средства и методы защиты беспилотных авиационных систем» базируется на результатах обучения, полученных при изучении дисциплин: «Информационная безопасность», «Программное обеспечение систем управления беспилотными летательными аппаратами», «Программно-аппаратная архитектура беспилотных авиационных систем», «Конструкция беспилотных воздушных судов».

Дисциплина «Средства и методы защиты беспилотных авиационных систем» является обеспечивающей для Выполнения и защиты выпускной квалификационной работы.

Дисциплина «Средства и методы защиты беспилотных авиационных систем» изучается в 8 семестре.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс освоения дисциплины «Средства и методы защиты беспилотных авиационных систем» направлен на формирование следующих компетенций:

Код компетенции/ индикатора	Результат обучения: наименование компетенции, индикатора компетенции
УК-1	Способен осуществлять поиск, критический

Код компетенции/ индикатора	Результат обучения: наименование компетенции, индикатора компетенции
	анализ и синтез информации, применять системный подход для решения поставленных задач
ИД1ук1	Осуществляет поиск информации об объекте, определяет достоверность полученной информации, формирует целостное представление об объекте, а также о сущности и последствиях его функционирования.
ОПК-3	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
ИД1опк-3	Строит математические модели при решении научно-исследовательских задач.

Планируемые результаты изучения дисциплины:

Знать:
- основные информационные источники, содержащие термины и понятия, относящиеся к криптографии;
- математические основы современной криптографии; показатели и проблемы стойкости криптосистем;

Уметь:
- самостоятельно анализировать модели обеспечения информационной безопасности; самостоятельно выбирать и анализировать информацию из информационных источников ЗИ БАС.
- осуществлять программную реализацию криптографических алгоритмов;

Владеть:
- навыками использования криптографических методов;
- методами оценки эффективности криптографических систем.

4 Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 академических часа.

Наименование	Всего часов	Семестр
		8
Общая трудоемкость дисциплины	72	72
Контактная работа:	32,3	32,3
лекции	16	16
практические занятия	16	16

семинары	–	–
лабораторные работы	–	–
курсовой проект (работа)	–	–
Самостоятельная работа студента	31	31
Промежуточная аттестация	9	9
контактная работа	0,3	0,3
самостоятельная работа по подготовке к зачету	8,7	8,7

5 Содержание дисциплины

5.1 Соотнесения тем (разделов) дисциплины и формируемых компетенций

Темы (разделы) дисциплины	Количество часов	Компетенции		Образовательные технологии	Оценочные средства
		УК-1	ОПК-3		
Тема 1. Программные средства и методы защиты линий передачи данных и управления БАС.	15	+		ВК, ПЗ, СРС, Л	Д, УО
Тема 2. Технические средства и методы защиты линий передачи данных и управления БАС.	16	+		ПЗ, СРС, Л	Д, УО
Тема 3. Организация разнородного использования БАС в целях повышения безопасности управления и передачи данных.	16	+		ПЗ, СРС, Л	Д, УО
Тема 4. Средства и методы обнаружения и подавления БАС.	16	+		ПЗ, СРС, Л	Д, УО
Всего по дисциплине	63				
Промежуточная аттестация	9				
Итого по дисциплине	72				

ПЗ – практическое занятие, СРС – самостоятельная работа студента, ВК – входной контроль, П – проект, Д – доклад, Л – лекция, УО – устный опрос.

5.2 Темы (разделы) дисциплины и виды занятий

Наименование темы (раздела) дисциплины	Л	ПЗ	С	ЛР	СРС	КР	Всего часов
Тема 1. Программные средства и методы защиты линий передачи данных и управления БАС.	4	4	-	-	7	-	15
Тема 2. Технические средства и методы защиты линий передачи данных и управления БАС.	4	4	-	-	8	-	16
Тема 3. Организация разнородного использования БАС в целях повышения безопасности управления	4	4	-	-	8	-	16

Наименование темы (раздела) дисциплины	Л	ПЗ	С	ЛР	СРС	КР	Всего часов
и передачи данных.							
Тема 4. Средства и методы обнаружения и подавления БАС.	4	4			8		16
Всего по дисциплине	16	16	-	-	31	-	63
Промежуточная аттестация							9
Итого по дисциплине							72

Л – лекция, ПЗ – практическое занятие, СРС – самостоятельная работа студента, С – семинар, ЛР – лабораторная работа, КР – курсовая работа (проект).

5.3 Содержание дисциплины

Тема 1. Программные средства и методы защиты линий передачи данных и управления БАС.

Алгоритмы и методы защиты линий передачи данных и управления БАС. Программные средства защиты линий передачи данных и управления БАС.

Тема 2. Технические средства и методы защиты линий передачи данных и управления БАС.

Структура технической защиты линий передачи данных БАС. Технические средства защиты линий управления БАС.

Тема 3. Организация разнородного использования БАС в целях повышения безопасности управления и передачи данных.

Теоретические основы разнородного использования БАС в целях повышения безопасности управления и передачи данных. Построение систем разнородного использования БАС.

Тема 4. Средства и методы обнаружения и подавления БАС.

Антидроновые комплексы обнаружения и подавления БАС. Зарубежные антидроновые средства.

5.4 Практические занятия (семинары)

Номер темы дисциплины	Тематика практических занятий (семинаров)	Трудоемкость (часы)
1	Практическое занятие №1. Алгоритмы шифрования данных.	2
	Практическое занятие №2. Протоколы защищенной передачи данных.	2
2	Практическое занятие №3. Моделирование сигналов и помех в системах связи.	2
	Практическое занятие №4. Моделирование сигналов и помех в системах связи.	2

3	Практическое занятие №5. Моделирование разнородной сети передачи данных.	2
	Практическое занятие №6. Моделирование разнородной сети передачи данных.	2
4	Практическое занятие №7. Антидроновые системы и комплексы.	2
	Практическое занятие №8. Антидроновые системы и комплексы.	2
Итого по дисциплине:		16

5.5 Лабораторный практикум

Лабораторный практикум учебным планом не предусмотрен.

5.6 Самостоятельная работа

Номер темы дисциплины	Виды самостоятельной работы	Трудо-емкость (часы)
1	1. Поиск, анализ информации и проработка учебного материала [1, 2, 3]. 2. Подготовка к докладу.	7
2	1. Поиск, анализ информации и проработка учебного материала [1,4,5-14]. 2. Подготовка к проекту.	8
3	1. Поиск, анализ информации и проработка учебного материала [1,4,5-14]. 2. Подготовка к проекту.	8
4	3. Поиск, анализ информации и проработка учебного материала [1,4,5-14]. 4. Подготовка к проекту.	8
Итого по дисциплине		31

5.7 Курсовые работы (проекты)

Курсовые работы (проекты) учебным планом не предусмотрены.

6 Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Макаренко С. И. Противодействие беспилотным летательным аппаратам. [Электронный ресурс] : Монография. – СПб.: Наукоемкие технологии, 2020. – 204 с. - Режим доступа: https://www.researchgate.net/publication/346075919_Protivodejstvie_bespilotnym_letatelnym_apparatam_Counter_Unmanned_Aerial_Ve

hicles/link/5fba11d892851c933f4dca84/download. – Загл. с экрана. (дата обращения: 29.09.2023).

2. Фомичёв, В. М. **Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты** : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под ред. В. М. Фомичёва. — М. : Издательство Юрайт, 2017. — 209 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-01740-3. — Режим доступа : www.biblio-online.ru/book/A01C7E90-A5B7-4B50-B348-31CB49CA5B3D .

3. Фомичёв, В. М. **Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата** / В. М. Фомичёв, Д. А. Мельников; под ред. В. М. Фомичёва. — М.: Издательство Юрайт, 2018. — 245 с. — (Серия: Бакалавр. Академический курс). — ISBN 978-5-9916-7090-6. — Режим доступа : www.biblio-online.ru/book/AF99BBDE-AF3A-43A9-A90F-B99806553C25

4. Нестеров, С.А. **Основы информационной безопасности** [Электронный ресурс] : учебное пособие / С.А. Нестеров. — Электрон. дан. — Санкт-Петербург : Лань, 2018. — 324 с. — Режим доступа: https://e.lanbook.com/book/103908 . — Загл. с экрана.

б) дополнительная литература:

5. Васильева, И. Н. **Криптографические методы защиты информации** : учебник и практикум для академического бакалавриата / И. Н. Васильева. — М. : Издательство Юрайт, 2017. — 349 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-02883-6. — Режим доступа : www.biblio-online.ru/book/38C7E67F-676F-4A9E-8E92-FD548EA095BA .

6. **Введение в теоретико-числовые методы криптографии** [Электронный ресурс] : учебное пособие / М.М. Глухов [и др.]. — Электрон. дан. — Санкт-Петербург: Лань, 2011. — 400 с. — Режим доступа: https://e.lanbook.com/book/68466 . — Загл. с экрана .

7. Васильев, К. К. Математическое моделирование систем связи: учебное пособие / К. К. Васильев, М. Н. Служивый. – 2-изд., перераб. и доп. – Ульяновск : УлГТУ, 2010. – 170 с [Электронный ресурс] - Режим доступа: http://lib.ulstu.ru/venec/disk/2012/Vasiljev.pdf. – Загл. с экрана. (дата обращения: 29.09.2023).

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

8 **Математическая криптография** [Электронный ресурс]. – Режим доступа: http://cryptography.ru/ . – Загл. с экрана. (дата обращения: 29.09.2023).

9 **Видео материалы по моделированию систем в SimInTech**. [Электронный ресурс]. – Режим доступа: https://simintech.ru/science/publications/video/ .– Загл. с экрана. (дата обращения: 29.09.2023).

10 **Новый подход к защите воздушного пространства** [Электронный ресурс]. – Режим доступа: https://sky-x.pro/ . – Загл. с экрана. (дата обращения: 29.09.2023).

11 **Всё о беспилотной отрасли на одном ресурсе** [Электронный ресурс]. – Режим доступа: https://russiandrone.ru/. – Загл. с экрана. (дата обращения: 29.09.2023).

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

12 **Единое окно доступа к образовательным ресурсам** [Электронный ресурс]. – Режим доступа:http://window.edu.ru, свободный (дата обращения: 29.09.2023).
13 **Электронная библиотека научных публикаций «eLIBRARY.RU»** [Электронный ресурс] — Режим доступа: http://elibrary.ru/, свободный (дата обращения: 29.09.2023).
14 **Электронно-библиотечная система издательства «Лань»** [Электронный ресурс] — Режим доступа: http://e.lanbook.com/,свободный (дата обращения: 29.09.2023).
15 **Среда динамического моделирования SimInTech** [Электронный ресурс] — Режим доступа https://simintech.ru/ - свободный (дата обращения: 29.09.2023).
16 **Сайт библиотеки GNU MP** [Электронный ресурс] — Режим доступа: http://gmplib.org – свободный (дата обращения: 29.09.2023).
17 **Сайт библиотеки GNU Crypto** [Электронный ресурс] — Режим доступа: http://www.gnu.org/s/gnu-crypto - свободный (дата обращения: 29.09.2023).

7 Материально-техническое обеспечение дисциплины

Компьютерные классы кафедры № 8 с доступом в Интернет, переносной проектор.

Информационно-справочные и материальные ресурсы библиотеки СПбГУ ГА.

Лицензионное программное обеспечение: Microsoft Office, Cygwin, SimInTech, Linux, SMath Studio.

8 Образовательные и информационные технологии

Дисциплина «Средства и методы защиты беспилотных авиационных систем» предполагает использование следующих образовательных технологий: входной контроль, практические занятия и самостоятельная работа студента.

Входной контроль проводится преподавателем в начале изучения дисциплины с целью коррекции процесса усвоения студентами дидактических единиц. Он осуществляется по вопросам из дисциплин, на которых базируется дисциплина «Средства и методы защиты беспилотных авиационных систем» (п. 2).

Лекция составляет основу теоретического обучения в рамках дисциплины и направлена на систематизированное изложение накопленных и актуальных научных знаний. Лекция предназначена для раскрытия состояния и перспектив развития экономических знаний в современных условиях. На лекции концентрируется внимание обучающихся на наиболее сложных и узловых вопросах, стимулируется их активная познавательная деятельность.

Практическое занятие по дисциплине «Средства и методы защиты беспилотных авиационных систем» содействует выработке у обучающихся умений и навыков применения знаний, полученных в ходе самостоятельной работы. Практические занятия как образовательная технология помогает студентам систематизировать, закрепить и углубить знания.

Самостоятельная работа студента проявляется в систематизации, планировании, контроле и регулировании его учебно-профессиональной деятельности, а также собственные познавательно-мыслительные действия без непосредственной помощь и руководства со стороны преподавателя. Основной целью самостоятельной работы студента является формирование навыка самостоятельного приобретения им знаний по некоторым несложным вопросам теоретического курса, закрепление и углубление полученных знаний, умений и навыков во время практических занятий. Самостоятельная работа подразумевает выполнение студентом поиска, анализа информации, проработку на этой основе учебного материала, подготовку к докладу, а также подготовку проекта.

В рамках изучения дисциплины «Средства и методы защиты беспилотных авиационных систем» предполагается использовать в качестве информационных технологий среду Microsoft Office, Cygwin, SimInTech, Linux, SMath Studio.

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

Фонд оценочных средств дисциплины «Средства и методы защиты

беспилотных авиационных систем» представляет собой комплекс методических и контрольных измерительных материалов, предназначенных для определения качества результатов обучения и уровня сформированности компетенций обучающихся в ходе освоения данной дисциплины. В свою очередь, задачами использования фонда оценочных средств являются осуществление как текущего контроля успеваемости студентов, так и промежуточной аттестации в форме зачета.

Фонд оценочных средств дисциплины «Средства и методы защиты беспилотных авиационных систем» для текущего контроля включает: проект и доклад.

Доклад представляет собой публичное выступление по представлению полученных результатов анализа определенной учебно-исследовательской темы. Типовые темы докладов представлены в п. 9.4.

Устный опрос проводится на практических занятиях с целью контроля усвоения теоретического материала , излагаемого на лекции.

Промежуточная аттестация по итогам освоения дисциплины проводится в виде зачета в 8 семестре. Этот вид промежуточной аттестации позволяет оценить уровень освоения студентом компетенций за весь период изучения дисциплины. Зачет предполагает устные ответы на 2 теоретических вопроса из перечня вопросов, вынесенных на промежуточную аттестацию, а также решение задачи.

9.1 Балльно-рейтинговая оценка текущего контроля успеваемости и знаний студентов по дисциплине

Не применяется.

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

Устный опрос оценивается следующим образом:

«зачтено»: обучающийся дает ответ на поставленный вопрос по существу и правильно отвечает на уточняющие вопросы;

«не зачтено»: обучающийся отказывается отвечать на поставленный вопрос, либо отвечает на него неверно и при формулировании дополнительных (вспомогательных) вопросов.

Решение ситуационных задач оценивается:

«зачтено»: обучающийся самостоятельно правильно решает задачу, дает обоснованную оценку по итогу решения;

«не зачтено»: обучающийся отказывается от выполнения задачи или не способен ее решить самостоятельно, а также с помощью преподавателя.

Доклад:

«зачтено»: грамотное и непротиворечивое изложение сути вопроса при использовании современных источников. Обучающийся способен сделать обоснованные выводы, а также уверенно отвечать на заданные в ходе обсуждения вопросы;

«не зачтено»: неудовлетворительное качество изложения материала и неспособность обучающегося сделать обоснованные выводы или рекомендации.

Письменная аудиторная работа:

«зачтено»: работа зачитывается в том случае, если задание выполнено полностью, в соответствии с поставленными требованиями и сделаны необходимые выводы;

«не зачтено»: работа не зачитывается в том случае, если обучающийся не выполнил задания, или результат выполнения задания не соответствует поставленным требованиям, а в заданиях и (или) ответах имеются существенные ошибки.

По итогам освоения дисциплины «Средства и методы защиты беспилотных авиационных систем» проводится аттестация обучающихся в форме зачета и предполагает решение задач на компьютере по билетам на практические вопросы из перечня.

Зачет является заключительным этапом изучения дисциплины «Средства и методы защиты беспилотных авиационных систем» и имеет целью проверить и оценить учебную работу студентов, уровень полученных ими знаний, умение применять их к решению практических задач, овладение практическими навыками в объеме требований образовательной программы на промежуточном этапе формирования компетенции ОПК – 3.

Во время подготовки к зачету студенты могут пользоваться материальным обеспечением, перечень которого утверждается заведующим кафедры.

На подготовку к ответу студенту предоставляется до 60 минут. По готовности к ответу или по вызову экзаменатора студент предъявляет решенные на зачете задачи. После ответа студента экзаменатор имеет право задать ему дополнительные вопросы в объеме учебной программы.

В итоге проведенного зачета студенту выставляется зачет/незачет. Экзаменатор несет личную ответственность за правильность выставленного зачета и оформления зачетной ведомости и зачетной книжки.

9.3 Темы курсовых работ (проектов) по дисциплине

Написание курсовых работ (проектов) учебным планом не предусмотрено.

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

1. Формальное определение алгоритма.

2. Пример вычислительной проблемы.

3. Формальное описание алгоритма. Отличия от кода языка высокого уровня.

4. Роль асимптотической нотации в определении производительности алгоритмов и структур данных.

5. Амортизационный анализ – назначение и примеры использования.

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

Критерий и показатели оценивания (индикаторы достижения) компетенций	Этапы формирования	Показатель
Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1), *Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-3)*		
Знать: – основные информационные источники, содержащие термины и понятия, относящиеся к ЗИ БАС;	1 этап формирования	– самостоятельно находит информационные источники, относящиеся к криптографическому анализу;
	2 этап формирования	– выделяет из имеющейся избыточной информации необходимую для решения поставленной задачи;
– математические основы современной криптографии; показатели и проблемы стойкости криптосистем	1 этап формирования	- называет основные классы криптосистем, простейшие шифры и их свойства;
	2 этап формирования	- строит математические модели шифров, классифицирует показатели стойкости криптосистем;
Уметь: – самостоятельно анализировать модели обеспечения информационной безопасности.	1 этап формирования	- воспроизводит модели обеспечения информационной безопасности
	2 этап формирования	- анализирует стратегии обеспечения информационной безопасности, оценивает защищенность процессов переработки информации;

Критерий и показатели оценивания (индикаторы достижения) компетенций	Этапы формирования	Показатель
– осуществлять программную реализацию криптографических алгоритмов	1 этап формирования	- составляет криптографические алгоритмы с использованием псевдокода и (или) блок-схем;
	2 этап формирования	- определяет криптографический алгоритм и составляет его с использованием заданного языка программирования;
Владеть: – навыками использования криптографических методов	1 этап формирования	- перечисляет основные криптографические задачи и методы их решения;
	2 этап формирования	– объясняет и применяет методы решения основных криптографических задач;
Владеть: - методами оценки эффективности криптографических систем	1 этап формирования	- перечисляет типы основных способов криптоанализа шифров, способы построения хеш-функций и основные требования к ним, основные типы электронной подписи и криптографических протоколов;
	2 этап формирования	– - анализирует эффективность хеш-функций, классифицирует основные типы электронной подписи, оценивает их эффективность.

Зачет

«зачтено» выставляется обучающемуся, если он даёт ответ на поставленный вопрос по существу и в надлежащем темпе, правильно отвечает на уточняющие вопросы; правильно управляет грамматическими структурами, демонстрирует словарный запас, достаточный для эффективного общения на общие темы.

«не зачтено» выставляется обучающемуся, если он отказывается отвечать на поставленный вопрос, либо отвечает на него, демонстрируя весьма ограниченный диапазон словаря, состоящий только из отдельных слов; неправильно управляя грамматическими структурами.

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

Типовые темы докладов:

6. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
7. Информация, основные свойства и характеристики безопасности ее применения.
8. Комплексное обеспечение информационной безопасности государства.

9. Области и объекты по обеспечению информационной безопасности и защите информационной деятельности.
10. Технологии обеспечения безопасности обработки информации.
11. Обеспечение информационной безопасности в нормальных и чрезвычайных ситуациях.

Перечень типовых вопросов к зачету для проведения промежуточной аттестации по дисциплине

1. Определение информационной безопасности.
2. Что такое доступность информации?
3. Какие возможные степени секретности Вы знаете?
4. Перечислите основные типы угроз информационной безопасности. Приведите примеры к каждому типу.
5. Какие основные эволюционные подходы к обеспечению информационной безопасности деятельности общества Вы знаете?
6. Сформулируйте основные проблемы информационной безопасности.
7. Каковы основные группы моделей безопасности?
8. Какие модели разграничения доступа Вы знаете?
9. Какие существуют критерии оценки защищенности объектов?
10. Алгоритм блочного шифрования DES и его модификации.
11. Алгоритм блочного шифрования AES. Алгоритм Rijndael.
12. Алгоритм блочного шифрования RC6.
13. Алгоритм блочного шифрования Safer.
14. Потоковое шифрование. Метод RC4.
15. Потоковое шифрование. Метод SEAL.
16. Потоковое шифрование. Метод WAKE.
17. Ассиметричная криптосистема шифрования Эль-Гамаля.
18. Криптосистема, основанная на проблеме Диффи-Хеллмана.
19. Алгоритмы цифровой электронной подписи.
20. Стандарты цифровой электронной подписи.
21. Функции хэширования. Достоинства и недостатки различных видов хэширования.

Типовая задача для промежуточной аттестации:

Описать (привести блок-схему или псевдокод) алгоритм симметричного шифрования. Режим выполнения алгоритма – простая замена.

10 Методические рекомендации для обучающихся по освоению дисциплины

Методика преподавания дисциплины «Средства и методы защиты беспилотных авиационных систем» характеризуется совокупностью методов, приемов и средств обучения, обеспечивающих реализацию содержания и учебно-воспитательных целей дисциплины, которая может быть представлена как некоторая методическая система, включающая методы, приемы и средства

обучения. Такой подход позволяет более качественно подойти к вопросу освоения дисциплины обучающимися.

Основными видами учебных занятий по дисциплине являются практические занятия. Объем и виды учебных занятий определены представленной рабочей программой дисциплины.

Практические занятия по дисциплине имеют целью:

- углубление, расширение и конкретизацию знаний, до уровня, на котором возможно их практическое использование;
- отработку навыков и умений в пользовании соответствующем математическим аппаратом.

Основу практических занятий составляет работа каждого обучаемого индивидуальная и (или) коллективная, по приобретению умений и навыков использования закономерностей, принципов, методов, форм и средств, составляющих содержание дисциплины в профессиональной деятельности и в подготовке к изучению дисциплин, формирующих компетенции выпускника.

По результатам контроля знаний и умений преподаватель должен провести анализ хода и итогов практических занятий, отметить успехи студентов в решении учебной задачи, а также недостатки и ошибки, разобрать их причины и дать методические указания к их устранению. Таким образом, практические занятия являются важной формой обучения, в ходе которых знания студентов превращаются в профессиональные необходимые умения, навыки.

Зачет являются заключительными оценочным средством, по итогам которого выявляется общий уровень овладения обучающимися предусмотренных компетенций по тематическим вопросам всего курса.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 01.03.04 «Прикладная математика».

Программа рассмотрена и утверждена на заседании кафедры №8 «Прикладной математики и информатики»

«28» сентября 2023 года, протокол № 2.

Разработчики:

к.п.н., доцент Самойлов В.А.

(ученая степень, ученое звание, фамилия и инициалы разработчиков)

И.о. заведующего кафедрой № 8 «Прикладной математики и информатики»

к.т.н. Земсков Ю.В.

(ученая степень, ученое звание, фамилия и инициалы заведующего кафедрой)

Программа согласована:

Руководитель ОПОП

д.т.н., доцент Костин Г.А.

(ученая степень, ученое звание, фамилия и инициалы руководителя ОПОП)

Программа рассмотрена и согласована на заседании Учебно-методического совета Университета «22» 11 2023 года, протокол № 3.