

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего
образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

УТВЕРЖДАЮ
Руководитель образовательной программы

доц., к.э.н., доц.
(должность, уч. степень, звание)

Т.Н. Елина
(инициалы, фамилия)
(подпись)

«20» февраля 2026 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Постквантовая криптография»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.04.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности/ специализации	Технологии искусственного интеллекта в информационной безопасности
Форма обучения	очная
Год приема	2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

зав.кафедрой, д.т.н., проф.
(должность, уч. степень, звание)

(подпись, дата)
20.02.26

С.В. Беззатеев
(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«20» февраля 2026 г, протокол № 7

Заведующий кафедрой № 33

д.т.н., проф.
(уч. степень, звание)

(подпись, дата)
20.02.26

С.В. Беззатеев
(инициалы, фамилия)

Заместитель директора института №3 по методической работе

доц., к.т.н.
(должность, уч. степень, звание)

(подпись, дата)
20.02.26

Н.В. Решетникова
(инициалы, фамилия)

Аннотация

Дисциплина «Постквантовая криптография» входит в образовательную программу высшего образования – программу специалитета по направлению подготовки/специальности 10.05.03 «Информационная безопасность автоматизированных систем» направленности/специализации «Безопасность открытых информационных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-2 «Способен формировать требования к защите информации в открытых информационных системах»

ПК-3 «Способен разрабатывать средства защиты сетей связи от несанкционированного доступа»

ПК-9 «Способен осуществлять работы по оценке работоспособности и эффективности применяемых программно-аппаратных средств защиты информации»

Содержание дисциплины охватывает круг вопросов, связанных с методами шифрования, используемыми в постквантовой криптографии, NP-сложными задачами, направлениями постквантовой криптографии, кодами, исправляющими ошибки, атаками на систему МакЭлиса.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа обучающегося, консультации.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме зачета (7 семестр).

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Получение обучающимися необходимых знаний и навыков в области вопросов, связанных с методами шифрования, используемыми в постквантовой криптографии, NP-сложными задачами, направлениями постквантовой криптографии, кодами, исправляющими ошибки, атаками на систему МакЭлиса.

1.2. Дисциплина входит в состав части, формируемой участниками образовательных отношений, образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Профессиональные компетенции	ПК-2 Способен формировать требования к защите информации в открытых информационных системах	ПК-2.3.1 знать основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях
Профессиональные компетенции	ПК-3 Способен разрабатывать средства защиты сетей связи от несанкционированного доступа	ПК-3.У.2 уметь решать типовые задачи помехоустойчивого кодирования и декодирования сообщений
Профессиональные компетенции	ПК-9 Способен осуществлять работы по оценке работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	ПК-9.3.4 знать криптографические алгоритмы и особенности их программной реализации ПК-9.У.1 уметь использовать приемы защитного программирования, защиты от типовых атак компьютерных систем

2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- Математический анализ
- Математическая логика и теория алгоритмов
- Физика
- Теория вероятностей и математическая статистика
- Вычислительная математика
- Технологии и методы программирования
- Математические основы обработки информации

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при изучении других дисциплин:

- Научно-исследовательская работа
- Защита информации в сенсорных сетях

3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№7
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	2/ 72	2/ 72
Из них часов практической подготовки	17	17
Аудиторные занятия, всего час.	51	51
в том числе:		
лекции (Л), (час)	34	34
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	17	17
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
Самостоятельная работа, всего (час)	21	21
Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Зачет,	Зачет,

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ)	ЛР (час)	КП (час)	СРС (час)
Семестр 7					
Раздел 1. Методы шифрования, используемые в постквантовой криптографии	8		5		4
Раздел 2. NP-сложные задачи	4		4		4
Раздел 3. Направления постквантовой криптографии	8				4
Раздел 4. Коды, исправляющие ошибки	8		4		4
Раздел 5. Атаки на систему МакЭлиса	6		4		5
Итого в семестре:	34		17		21
Итого	34	0	17	0	21

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Раздел 1. Методы шифрования, используемые в постквантовой криптографии Прямая схема. Двойственная схема. Multivariate Cryptography Треугольные отображения Lattice-based cryptography
2	Раздел 2. NP-сложные задачи Построение полиномиальных отображений в конечных полях. Хэш-функции, основанные на решетках Протокол обмена ключами
3	Раздел 3. Направления постквантовой криптографии Code based cryptography (основано на кодах исправляющих ошибки) Multivariate, quadratic equations cryptography (основано на многочленах в конечных полях) Lattice based cryptography (основано на теории решеток) Hash-based cryptography (основано на представлении хэш функций для больших данных)
4	Раздел 4. Коды, исправляющие ошибки
5	Раздел 5. Атаки на систему МакЭлиса

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено					
Всего					

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 7				
1	Задача А. Найти решение системы линейных диофантовых уравнений в целых числах	2	2	1
2	Задача Б. Найти решение системы полиномиальных уравнений в целых	3	3	1

	числах			
3	НР-сложные задачи	4	4	2
4	Коды, исправляющие ошибки	4	4	4
5	Атаки на систему МакЭлиса	4	4	5
Всего		17	17	

4.5. Выполнение курсового проекта/ курсовой работы
Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся
Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 7, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	10	10
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	5	5
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	6	6
Всего:	21	21

5. Перечень учебно-методического обеспечения
для самостоятельной работы обучающихся по дисциплине (модулю)
Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. разделов 6-11.

6. Перечень печатных и электронных учебных изданий
Перечень печатных и электронных учебных изданий приведен в таблице 8.
Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004.4 И 21	Иванова, Г. С. Технология программирования [Текст] : учебник / Г. С. Иванова. - М. : КноРус, 2011. - 333 с.	22
004 В 52	Вирт, Н. Алгоритмы и структуры данных. Новая версия для Оберона + CD [Текст] / Н. Вирт ; пер. Д. Б. Подшивалов. - 2-е изд., испр. - М. : ДМК Пресс, 2012. - 272 с.	10

004.4 Г 95	Гуриков, С. Р. Введение в программирование на языке Visual C# [Текст] : учебное пособие / С. Р. Гуриков. - М. : ФОРУМ : ИНФРА-М, 2013. - 448 с.	10
004 Л 85	Лупин, С. А. Технологии параллельного программирования [Текст] : учебное пособие / С. А. Лупин, М. А. Посыпкин. - М. : ФОРУМ: ИНФРА-М, 2015. - 208 с.	20
004.4 К 53	Кнут, Д. Искусство программирования [Текст] = The art of computer programming : [в 3 т.]. Т. 1. Основные алгоритмы / Д. Кнут ; ред. Ю. В. Козаченко. - 3-е изд. - М. : Вильямс, 2014. - 720 с.	5
004.4 К 84	Крук, Евгений Аврамович (проф.). Методы программирования и прикладные алгоритмы [Текст] : учебное пособие в 3 ч. Ч. 1 / Е. А. Крук, А. А. Овчинников ; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2014. - 178 с.	45
004.4 К 36	Керниган, Б. В. Язык программирования C [Текст] = The C programming language : пер. с англ. / Б. В. Керниган, Д. Ритчи. - 2-е изд., перераб. и доп. - М. и др. : Вильямс, 2016. - 288 с.	10
004.4 П 21	Пахомов, Б. И. C/C++ и MS Visual C++ для начинающих 2012 [Текст] / Б. И. Пахомов. - 2-е изд. - СПб. : БХВ - Петербург, 2015. - 528 с.	10
004.4 Э 38	Эккель, Брюс. Философия Java [Текст] / Б. Эккель. - 4-е изд. - СПб. : ПИТЕР, 2011. - 637 с.	1
004.4 С 28	Седжвик, Р. Алгоритмы на C++ : анализ структуры данных, сортировка, поиск, алгоритмы на графах [Текст] / Р. Седжвик ; конс. К. Ван Вик. - М. : Вильямс, 2014. - 1056 с.	5
004.4 О-66	Орлов, С. А. Теория и практика языков программирования [Текст] : учебник для бакалавров и магистров / С. А. Орлов. - СПб. : ПИТЕР, 2014. - 688 с.	5
004.4 Т 70	Троелсен, Э. Язык программирования C# 5.0 и платформа .NET 4.5 [Текст] = Pro C# 5.0 and the .NET 4.5 framework / Э. Троелсен. - 6-е изд. - М. и др. : Вильямс, 2015. - 1312 с.	2

7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
https://pro.guap.ru/	Материалы для выполнения практических работ, индивидуальные варианты для их выполнения, а также электронный лекционный материал по дисциплине размещаются внутри ЭИОС ГУАП «Интегрированная среда обучения» в течение учебного семестра

8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
1	Электронная информационно-образовательная среда ГУАП «Интегрированная среда обучения» (https://pro.guap.ru/) разработана сотрудниками ГУАП (введена в эксплуатацию приказом ГУАП от 06.06.2017 № 05-215/17), перечень модулей и их функциональное назначение изложены по ссылке https://guap.ru/it/system/iso
2	Официальный сайт образовательной организации в сети «Интернет» (https://guap.ru/), разработан сотрудниками ГУАП (введен в эксплуатацию Приказом ГУАП от 23.03.2023 № 05-145/23)
3	LibreOffice 5 (Лицензия LGPLv3)

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
1	ЭБС Znanium (https://znanium.ru/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП
2	ЭБС «Лань» (https://e.lanbook.com/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП
3	Электронный каталог библиотеки ГУАП с доступом к базе полнотекстовых изданий (https://lib.guap.ru), доступ через личный кабинет читателя библиотеки ГУАП

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Мультимедийная лекционная аудитория:	

	Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; набор демонстрационного оборудования. Обеспечен доступ в электронную информационно-образовательную среду ГУАП по точке доступа Wi-Fi.	
2	Лаборатория компьютерного моделирования: – специализированная мебель; – технические средства обучения, служащие для представления учебной информации; панель интерактивная/телевизор; Лабораторное оборудование: ПЭВМ – «Место рабочее автоматизированное» – 13 шт. Обеспечен доступ в электронную информационно-образовательную среду ГУАП по локальной вычислительной сети.	52-46, 52-44 (ул. Большая Морская, д.67, лит. А)
3	Помещение для самостоятельной работы, Интернет-класс. Специализированная мебель, возможность подключения к сети «Интернет» и доступ в электронную информационно-образовательную среду организации. 10 ПК, Принтер лазерный HPLJP4515n, Принтер HP LaserJetEnterprise 600 M602dn.	14-34 (ул. Большая Морская, д.67, лит. А)
4	Помещение для самостоятельной работы обучающихся - Читальный зал библиотеки ГУАП: специализированная мебель; персональные компьютеры – 10 шт., обеспечен доступ в электронную информационно-образовательную среду ГУАП по локальной вычислительной сети и точке доступа WiFi, а также к электронно-библиотечным системам, реферативной базе данных Scopus; копировальный аппарат Kyocera KM2035	22-19 (ул. Большая Морская, д.67, лит. А)

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Зачет	Список вопросов; Тесты; Задачи.

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 – Критерии оценки уровня сформированности компетенций

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	Обучающийся: – глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно связывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий. – правильно выполнил от 90% до 100% тестовых заданий ^{**} .
«хорошо» «зачтено»	Обучающийся: – твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий. – правильно выполнил от 70% до 89% тестовых заданий ^{**} .
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий. – правильно выполнил от 51% до 69% тестовых заданий ^{**} .
«неудовлетворительно» «не зачтено»	– обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений. – правильно выполнил менее 51% тестовых заданий ^{**} .

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
	Учебным планом не предусмотрено	

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
1	Прямая схема. Двойственная схема. Multivariate Cryptography	ПК-2.3.1

2	Треугольные отображения Lattice-based cryptography	ПК-3.У.2
3	Построение полиномиальных отображений в конечных полях. Хэш-функции, основанные на решетках Протокол обмена ключами	ПК-9.3.4
4	Code based cryptography (основано на кодах исправляющих ошибки) Multivariate, quadratic equations cryptography (основано на многочленах в конечных полях) Lattice based cryptography (основано на теории решеток) Hash-based cryptography (основано на представлении хэш функций для больших данных) Коды, исправляющие ошибки Атаки на систему МакЭлиса	ПК-9.У.1

Перечень тем для выполнения курсового проекта/ курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для выполнения курсового проекта / курсовой работы

№ п/п	Примерный перечень тем для выполнения курсового проекта/ курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
1	Вопрос 1 Какая главная угроза исходит от квантовых компьютеров для классической криптографии? 1. Увеличение длины ключа шифрования 2. Алгоритм Шора для разложения на множители и дискретного логарифмирования 3. Замедление скорости работы процессоров 4. Полная отмена симметричного шифрования • Правильный ответ: 2 Вопрос 2 Какой симметричный алгоритм считается относительно безопасным от атак квантового компьютера при условии удвоения длины ключа? 1. DES 2. RSA-2048 3. AES-256 4. RC4 • Правильный ответ: 3 Вопрос 3 На чем основана безопасность решеточных (lattice-based) криптосистем? 1. На сложности задачи о кратчайшем векторе в решетке (SVP) 2. На разложении больших чисел	ПК-2.3.1

	3. На дискретном логарифмировании в эллиптических кривых 4. На хэш-функциях • Правильный ответ: 1	
2	Вопрос 4 Какой из алгоритмов основан на теории решеток и выбран NIST в качестве основного стандарта для общего шифрования? 2. Classic McEliece 3. CRYSTALS-Kyber 4. SPHINCS+ • Правильный ответ: 3 Вопрос 5 На чем основана криптография на основе кодов (code-based)? 1. На трудных задачах теории линейных кодов, исправляющих ошибки 2. На изогениях суперсингулярных эллиптических кривых 3. На свойствах многочленов от многих переменных 4. На дискретном логарифмировании • Правильный ответ: 1 Вопрос 6 Какой классический код лежит в основе криптосистемы МакЭлиса (McEliece)? 1. Код Хемминга 2. Код Рида-Соломона 3. Двоичный код Галлагера 4. Полноразмерный код Гёппы • Правильный ответ: 4	ПК-3.У.2
3	Вопрос 7 На чем основана многомерная (multivariate) криптография? 1. На решении систем нелинейных квадратных уравнений над конечным полем 2. На задаче о рюкзаке 3. На хэш-деревьях 4. На свойствах простых чисел • Правильный ответ: 1 Вопрос 8 Какое главное преимущество имеют многомерные схемы подписи (например, Rainbow)? 1. Очень маленькая длина открытого ключа 2. Высокая скорость создания подписи 3. Полное отсутствие математических уязвимостей 4. Маленький размер самой подписи • Правильный ответ: 2 Вопрос 9 На чем основана криптография на основе хэш-функций (hash-based signatures)? 2. На безопасности базовых хэш-функций (SHA-2, SHA-3) 3. На задаче целочисленного деления 4. На обращении матриц • Правильный ответ: 2	ПК-9.3.4
4	Вопрос 10 Какой пример относится к хэш-подписям с состоянием (stateful hash-based)?	ПК-9.У.1

1. XMSS (eXtended Merkle Signature Scheme) 2. CRYSTALS-Dilithium 3. Falcon 4. RSA • Правильный ответ: 1 Вопрос 11 На чем основана криптография на основе изогений (isogeny-based)? 1. На поиске путей изогений между суперсингулярными эллиптическими кривыми 2. На сложности умножения матриц 3. На переборе хэш-сумм 4. На факторизации полиномов • Правильный ответ: 1 Вопрос 12 Какой протокол на изогениях долгое время привлекал внимание из-за крошечных ключей, но пострадал от серьезной атаки в 2022 году? 1. SIKE (Supersingular Isogeny Key Encapsulation) 2. Kyber 3. Dilithium 4. McEliece • Правильный ответ: 1	
--	--

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

11. Методические указания для обучающихся по освоению дисциплины

11.1. Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимся лекционного материала:

- получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;
- получение опыта творческой работы совместно с преподавателем;

- развитие профессионально–деловых качеств, любви к предмету и самостоятельного творческого мышления.
- появление необходимого интереса, необходимого для самостоятельной работы;
- получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);
- получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

Раздел 1. Методы шифрования, используемые в постквантовой криптографии

Раздел 2. NP-сложные задачи

Раздел 3. Направления постквантовой криптографии

Раздел 4. Коды, исправляющие ошибки

Раздел 5. Атаки на систему МакЭлиса

–

11.2. Методические указания для обучающихся по прохождению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

- приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;
- закрепление, развитие и детализация теоретических знаний, полученных на лекциях;
- получение новой информации по изучаемой дисциплине;
- приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ (ЛР)

- В задании должно быть четко сформулирована задача, выполняемая в ЛР;
- Описаны входные и выходные данные для проведения ЛР;
- ЛР должна выполняться на основе полученных теоретических знаниях;
- Выполнение ЛР должно осуществляться на основе методических указаний, предоставляемых преподавателем;
- ЛР должна выполняться в специализированном компьютерном классе и может быть доработана студентом в домашних условиях, если позволяет ПО;
- Итогом выполненной ЛР является отчет.

Структура и форма отчета о лабораторной работе

- Постановка задачи;

- Входные и выходные данные;
- Содержание этапов выполнения;
- Обоснование полученного результата (вывод);
- Список используемой литературы.

Требования к оформлению отчета о лабораторной работе

- Лабораторная работа (ЛР) предоставляется в печатном/или электронном виде;
- ЛР должна соответствовать структуре и форме отчета представленной выше;
- ЛР должна иметь титульный лист (ГОСТ 7.32-2001 издания 2008 года) с названием и подписью студента(ов), который(ые) ее сделал(и) и оформил(и);

Студент должен защитить ЛР. Отметка о защите должна находиться на титульном листе вместе с подписью преподавателя.

11.3. Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

В процессе выполнения самостоятельной работы у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет ему развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

11.4. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

Текущий контроль включает следующие формы:

- Устный опрос (коллоквиум, собеседование)
- Письменные работы (тестирование)
- Лабораторные работы
- Проектная деятельность (рефераты, доклады, презентации)

Критерии оценивания

Оценка выставляется на основе демонстрации обучающимся следующих компетенций:

- Оценка «Отлично» (высокий уровень): глубокое знание материала, логичное изложение, умение решать нестандартные задачи, аргументированные ответы.
- Оценка «Хорошо» (продвинутый уровень): твердое знание материала, грамотное изложение, выполнение практических заданий без принципиальных ошибок, небольшие неточности при ответах.

- Оценка «Удовлетворительно» (пороговый уровень): знание базовых положений, затруднения при самостоятельном анализе, наличие ошибок в вычислениях или логике, неуверенные ответы.

- Оценка «Неудовлетворительно» (критический уровень): отсутствие базовых знаний, невыполнение обязательных практических заданий, отказ от ответа.

Порядок ликвидации задолженностей

- Обучающийся обязан проходить все формы контроля в установленные сроки.
- В случае пропуска по уважительной причине (болезнь, подтвержденная справкой), сроки прохождения переносятся.

- При неудовлетворительной оценке или неуважительном пропуске обучающийся обязан отработать задолженность в часы консультаций преподавателя до начала сессии.

11.5. Методические указания для обучающихся по прохождению промежуточной аттестации.

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

- зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

Основные этапы сдачи зачета

1. Получение допуска

Перед зачетом студент должен выполнить минимальные учебные требования:

- Посетить обязательные практические и лабораторные занятия.
- Сдать все текущие работы (рефераты, отчеты, контрольные).
- Закрывать академические долги по текущей успеваемости.

2. Подготовка к зачету

Преподаватель заранее выдает материалы для подготовки:

- Вопросы к зачету (список утверждается на кафедре).
- Список основной и дополнительной литературы.
- Типовые практические задачи или кейсы.

3. Проведение процедуры

Сдача проходит по утвержденному расписанию в форме:

- Устная форма: студент тянет билет, готовится (20–40 минут) и отвечает преподавателю.

4. Выставление оценки

Результат фиксируется сразу после ответа или проверки работы:

- Преподаватель ставит отметку «зачтено» или «не зачтено».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой