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

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

С.В. Беззатеев
(инициалы, фамилия)

(подпись)

«20» февраля 2026 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Базовое представление о протоколах квантового распределения ключей»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.05.03
Наименование направления подготовки/ специальности	Информационная безопасность автоматизированных систем
Наименование направленности/ специализации	Безопасность открытых информационных систем
Форма обучения	очная
Год приема	2026

Санкт-Петербург– 2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

зав.кафедрой, д.т.н.,проф.	20.02.26	С.В. Беззатеев
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33
«20» февраля 2026 г, протокол № 7

Заведующий кафедрой № 33

д.т.н.,проф.	20.02.26	С.В. Беззатеев
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №3 по методической работе

доц.,к.т.н.	20.02.26	Н.В. Решетникова
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Аннотация

Дисциплина «Базовое представление о протоколах квантового распределения ключей» 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 не является обязательной при освоении обучающимся образовательной программы и направлена на углубленное формирование следующих компетенций:

ПК-4 «Способен осуществлять работы по разработке систем защиты информации автоматизированных систем»

Содержание дисциплины охватывает круг вопросов, связанных с изучением физических основ квантовой механики, принципов работы криптографических протоколов (таких как BB84 и E91) и обеспечением информационной безопасности.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельная работа обучающегося.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме зачета (4 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 - формирование у студентов фундаментальных теоретических знаний и практических представлений о принципах создания гарантированно защищенных симметричных ключей шифрования с использованием законов квантовой физики.

1.2. Дисциплина является факультативной дисциплиной по специальности 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-4 Способен осуществлять работы по разработке систем защиты информации автоматизированных систем	ПК-4.З.3 знать критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем ПК-4.У.3 уметь выбирать меры защиты информации, подлежащие реализации в открытой автоматизированной системе ПК-4.В.2 владеть навыками разработки предложений по совершенствованию системы управления безопасностью информации в открытых информационных системах

2. Место дисциплины в структуре ОП

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

– «Информатика»,

– «Основы программирования»,

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

– «Основы квантовых алгоритмов в защите информации»,

– « Математические модели квантовых вычислений»

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
		№4
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	2/ 72	2/ 72
Из них часов практической подготовки	17	17
Аудиторные занятия, всего час.	34	34
в том числе:		

лекции (Л), (час)	17	17
практические/семинарские занятия (ПЗ), (час)	17	17
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
Самостоятельная работа, всего (час)	38	38
***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) (час)	ЛР (час)	КП/КР (час)	СР (час)
Семестр 4					
Раздел 1. Физико-математические основы квантовой информатики Тема 1.1. Введение в квантовые технологии и постулаты квантовой механики. Тема 1.2. Понятие кубита (q-bit), сфера Блоха и суперпозиция состояний. Тема 1.3. Квантовые измерения, теорема о запрете клонирования неизвестного квантового состояния. Тема 1.4. Матрица плотности и квантовая запутанность (ЭПР-пары).	4	4			8
Раздел 2. Базовые протоколы квантового распределения ключей (КРК) Тема 2.1. Четырехпозиционный протокол BB84: кодирование, смена базисов, перехват (атака Intercept-Resend). Тема 2.2. Двухпозиционный протокол B92 и его уязвимости. Тема 2.3. Протокол E91 (Эккерта) на основе квантовой запутанности и проверка неравенств Белла. Тема 2.4. Другие типы кодирования: фазовое, временное (Time-Bin) и многоуровневые системы.	4	4			10
Раздел 3. Этапы классической постобработки в КРК Тема 3.1. Оценка уровня квантовых ошибок в канале связи (QBER). Тема 3.2. Процедура исправления ошибок (протоколы Cascade, Winnow или LDPC-коды). Тема 3.3. Усиление секретности (Privacy Amplification) и сжатие информации с помощью хеш-функций.	4	4			10

Раздел 4. Аппаратная реализация и угрозы информационной безопасности Тема 4.1. Компоненты систем КРК: источники одиночных фотонов, волоконно-оптические линии, детекторы (SPAD, SNSPD). Тема 4.2. Ограничения по дальности: затухание в оптическом волокне и концепция квантовых повторителей. Тема 4.3. Атаки на физическую реализацию систем КРК (Trojan-horse attack, blinding attack) и методы противодействия.	5	5			10
Итого в семестре:	17	17			38
Итого	17	17	0	0	38

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
	Раздел 1. Физико-математические основы квантовой информатики Раздел посвящен изучению базового математического аппарата и физических законов, на которых строится квантовая криптография. Студенты осваивают концепцию кубита как фундаментальной единицы информации, изучают геометрическое представление состояний на сфере Блоха и принцип суперпозиции. Особое внимание уделяется фундаментальным запретам квантового мира: невозможности скопировать неизвестное состояние (теорема о запрете клонирования) и разрушению исходного состояния при попытке его измерения. Также рассматривается феномен квантовой запутанности и его математическое описание. Раздел 2. Базовые протоколы квантового распределения ключей (КРК) В рамках раздела детально разбирается логика работы основных криптографических алгоритмов, использующих квантовые каналы. Изучается классический протокол BB84, включая этапы кодирования состояний фотонов, выбора базисов отправителем (Алисой) и получателем (Бобом), а также процедуру просеивания ключа. Анализируется альтернативный двухпозиционный протокол B92 и протокол E91, использующий запутанные ЭПР-пары и проверку неравенств Белла для контроля целостности канала. Рассматриваются различные физические способы кодирования информации (поляризационное, фазовое, временное). Раздел 3. Этапы классической постобработки в КРК

	Раздел описывает обязательные математические процедуры, которые выполняются по открытому классическому каналу связи после завершения квантового сеанса. Студенты изучают методику расчета уровня ошибок (QBER), который позволяет обнаружить присутствие шпиона (Евы). Рассматриваются алгоритмы поиска и исправления неизбежных шумов в оптическом канале (интерактивный протокол Cascade, LDPC-коды). Заключительная часть раздела посвящена процедуре усиления секретности (Privacy Amplification), которая сжимает ключ с помощью хеш-функций, сводя к нулю любые частичные знания злоумышленника о полученной последовательности. Раздел 4. Аппаратная реализация и угрозы информационной безопасности Раздел связывает теоретические модели с практической инженерией и реальными технологиями. Изучается устройство современных систем КРК: лазерные источники, лавинные фотодиоды и сверхпроводниковые детекторы одиночных фотонов. Рассматриваются физические ограничения систем, такие как затухание сигнала в волокне, и способы увеличения дистанции связи (квантовые повторители). Важное место занимает анализ «уязвимостей реализации» — атак, направленных не на математику протокола, а на несовершенство оборудования (например, ослепление детекторов или зондирование троянским конем), и инженерные методы защиты от них.

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
Семестр 4					
1	Математическое описание кубита и расчет вероятностей квантовых измерений.	Семинар-практикум (аналитическое решение задач у доски, расчет матриц плотности и векторов состояний с использованием линейной алгебры).	4		1
2	Моделирование сеанса связи по протоколу BB84 и анализ атаки «перехват-повторная посылка».	Работа на симуляторе (работа в интерактивной программной среде, где студенты вручную или с помощью скриптов	4		2

		имитируют действия Алисы, Боба и Евы, рассчитывая итоговый просеянный ключ).			
3	Оценка параметра QBER и реализация алгоритмов исправления ошибок Cascade.	Практическое занятие по программированию (написание кода на Python для симуляции классического канала, поиска позиций с ошибками и применения хеш-функций для усиления секретности).	4		3
4	Аппаратная реализация и угрозы информационной безопасности Название занятия: Инженерный расчет оптического бюджета квантовой линии связи и анализ физических уязвимостей систем КРК.	Кейс-стади / Защита мини-проектов (анализ реальных технических спецификаций оборудования, расчет максимальной дальности связи с учетом затухания и разбор сценария конкретной атаки на детекторы с предложением мер защиты).	5		4
Всего			17		

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
Учебным планом не предусмотрено				
Всего				

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 4, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	20	20
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	9	9
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	9	9
Всего:	38	38

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)
https://e.lanbook.com/book/426110 (дата обращения: 12.02.2026). Режим доступа: для авториз. пользователей.	Филиппов, Ф. В. Квантовые вычисления : учебное пособие / Ф. В. Филиппов. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2024. — 83 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/426110 (дата обращения: 03.08.2026). — Режим доступа: для авториз. пользователей.	
https://e.lanbook.com/book/499784 (дата обращения: 12.02.2026). Режим доступа: для авториз.	Филиппов, Ф. В. Квантовые вычисления на Python : учебное пособие / Ф. В. Филиппов. —	

пользователей.	Вологда : Инфра-Инженерия, 2025. — 108 с. — ISBN 978-5-9729-2474-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/499784 (дата обращения: 03.08.2026). — Режим доступа: для авториз. пользователей.	
https://e.lanbook.com/book/426116 (дата обращения: 12.02.2026). Режим доступа: для авториз. пользователей.	Кирилюк, М. А. Квантовые вычисления для решения задач искусственного интеллекта : учебное пособие / М. А. Кирилюк, Н. А. Бочаров. — Москва : РТУ МИРЭА, 2026. — 95 с. — ISBN 978-5-7339-2874-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/523260 (дата обращения: 03.08.2026). — Режим доступа: для авториз. пользователей.	
https://e.lanbook.com/book/432662 (дата обращения: 12.02.2026). Режим доступа: для авториз. пользователей.	Сысоев, С. С. Введение в квантовые вычисления. Квантовые алгоритмы : учебное пособие / С. С. Сысоев. — Санкт-Петербург : СПбГУ, 2019. — 144 с. — ISBN 978-5-288-05933-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/505514 (дата обращения: 03.08.2026). — Режим доступа: для авториз. пользователей.	
https://e.lanbook.com/book/505514 (дата обращения: 12.02.2026). Режим доступа: для авториз. пользователей.	Масленников, В. В. Введение в квантовые вычисления : учебное пособие / В. В. Масленников. — Москва : РТУ МИРЭА, 2024. — 74 с. — ISBN 978-5-7339-2254-6. — Текст : электронный // Лань : электронно-библиотечная	

	система. — URL: https://e.lanbook.com/book/432662 (дата обращения: 03.08.2026). — Режим доступа: для авториз. пользователей.	
https://e.lanbook.com/book/523260 (дата обращения: 12.02.2026). Режим доступа: для авториз. пользователей.	Филиппов, Ф. В. Квантовые вычисления: лабораторный практикум : учебное пособие / Ф. В. Филиппов. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2024. — 42 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/426116 (дата обращения: 03.08.2026). — Режим доступа: для авториз. пользователей.	

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	Образовательная платформа «Юрайт» (https://urait.ru/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП
2	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	Компьютерный класс	52-44 Большая Морская,67.
2	Аудитории для самостоятельной подготовки	14-34 Большая Морская,67
3	Лекционная аудитория	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средствдля 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	В чем заключается фундаментальное отличие классического бита от квантового бита (кубита)? Дайте геометрическое описание кубита с помощью сферы Блоха. Что представляют собой точки на ее поверхности и	ПК-4.З.3

	внутри нее? Сформулируйте принцип квантовой суперпозиции и приведите пример его проявления. Сформулируйте и докажите (или обоснуйте) теорему о запрете клонирования неизвестного квантового состояния. Почему она важна для криптографии? Что такое квантовое измерение и как оно влияет на измеряемую квантовую систему? Что понимается под квантовой запутанностью (состояниями ЭПР)? Приведите пример запутанного состояния двух кубитов.	
2	Опишите пошаговый алгоритм работы протокола BB84 (действия Алисы и Боба). Что такое «просеивание ключа» в протоколе BB84 и на каком этапе оно происходит? Объясните суть атаки «перехват — повторная посылка» (Intercept-Resend). К какому уровню ошибок в протоколе BB84 приводит эта атака? В чем заключается главное отличие двухпозиционного протокола B92 от четырехпозиционного BB84? В чем его уязвимость? Опишите принцип работы протокола E91 (Эккерта). Как в нем используется квантовая запутанность? Какую роль играют неравенства Белла в протоколе E91 и как их нарушение гарантирует отсутствие шпиона в канале? Назовите основные физические степени свободы фотона, используемые для кодирования информации в КРК (поляризационное, фазовое, временное кодирование). Что такое параметр QBER (Quantum Error Bit Rate)? Как Алиса и Боб оценивают его величину? Какое пороговое значение QBER принято считать критическим для протокола BB84, после которого ключ отбраковывается? Почему? Зачем нужен этап исправления ошибок (Error Correction) и почему он выполняется по открытому классическому каналу? Опишите общую логику работы интерактивного алгоритма исправления ошибок Cascade. Что такое «усиление секретности» (Privacy Amplification) и какую задачу решает этот этап постобработки? Как именно применение хеш-функций на этапе усиления секретности уменьшает знания злоумышленника о итоговом ключе?	ПК-4.У.3
3	Назовите основные компоненты физического уровня системы КРК и их назначение. В чем разница между лавинными фотодиодами (SPAD) и сверхпроводниковыми детекторами одиночных фотонов (SNSPD)? Почему в реальных системах КРК вместо идеальных одиночных фотонов часто используют ослабленные лазерные импульсы? К какой уязвимости это приводит (атака PNS)? Какие факторы ограничивают максимальную дальность и скорость генерации ключа в волоконно-оптических линиях связи? Что такое квантовые повторители и почему для увеличения дальности КРК нельзя использовать обычные	ПК-4.В.2

	оптические усилители? Что представляют собой «атаки на физическую реализацию» (Side-Channel Attacks)? Приведите пример атаки типа «троянский конь» или «ослепление детекторов».	

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	Какое фундаментальное свойство квантовой механики делает невозможным незаметное копирование квантового ключа злоумышленником? 1. Закон сохранения энергии 2. Теорема о запрете клонирования 3. Принцип относительности 4. Эффект Доплера Верный ответ: 2 Что происходит с квантовым состоянием фотона при попытке злоумышленника измерить его в процессе передачи? 1. Состояние уничтожается без возможности фиксации 2. Состояние копируется в идеальную точность 3. Состояние неизбежно искажается (изменяется) 4. Состояние усиливается по мощности Верный ответ: 3 Как называется минимальная единица квантовой информации, используемая в протоколах квантовой криптографии? 1. Бит 2. Кубит 3. Байт 4. Триггер Верный ответ: 2 В каком из перечисленных протоколов квантового распределения ключей безопасность основана на использовании квантовой запутанности и проверке неравенств Белла? 1. BB84 2. B92 3. E91 4. COW Верный ответ: 3	ПК-4.3.3

2	Что делают отправитель (Алиса) и получатель (Боб) на этапе «просеивания» ключа в протоколе BB84? 1. Сравнивают сами значения отправленных и полученных битов 2. Сравнивают типы использованных базисов для каждого бита 3. Исправляют ошибки с помощью кодов 4. Проводят хеширование полученной строки Верный ответ: 2 К какому результату приводит атака «перехват — повторная посылка» (Intercept-Resend) со стороны шпиона в протоколе BB84? 1. К полной незаметной краже ключа 2. К блокировке классического канала связи 3. К появлению неизбежного уровня ошибок в просеянном ключе 4. К ускорению передачи данных Верный ответ: 3 Что измеряет параметр QBER в системах квантового распределения ключей? 1. Скорость генерации сырого ключа 2. Уровень квантовых ошибок в ключе 3. Длину волны лазерного излучения 4. Время задержки импульса в волокне Верный ответ: 2 По какому каналу связи выполняются этапы исправления ошибок и усиления секретности (классическая постобработка)? 1. По квантовому оптическому каналу 2. По открытому классическому каналу связи 3. По закрытому спутниковому каналу 4. Эти этапы выполняются без связи между легитимными пользователями Верный ответ: 2	ПК-4.У.3
3	Какая процедура постобработки используется для того, чтобы свести к нулю любые частичные знания злоумышленника о сформированном ключе? 1. Просеивание ключа 2. Исправление ошибок (Cascade) 3. Усиление секретности (Privacy Amplification) 4. Калибровка детекторов Верный ответ: 3 Почему для увеличения дальности квантовой связи нельзя использовать стандартные оптические усилители, применяемые в обычных линиях связи? 1. Усилители слишком сильно замедляют сигнал 2. Усилители меняют цвет (длину волны) фотонов 3. Усилители разрушают квантовые состояния из-за клонирования/шума 4. Усилители работают только с медными проводами Верный ответ: 3	ПК-4.В.2

	К какому типу уязвимостей относятся атаки типа «троянский конь» и «ослепление детекторов»? 1. К математическим уязвимостям самих протоколов 2. К атакам на физическую реализацию (аппаратное обеспечение) 3. К уязвимостям алгоритмов классического шифрования 4. К атакам на программное обеспечение серверов Верный ответ: 2 Какое техническое решение разрабатывается для преодоления ограничения по дальности передачи ключа в радиальных квантовых сетях без раскрытия секретности на промежуточных узлах? 1. Оптические разветвители 2. Квантовые повторители (репитеры) 3. Более мощные классические лазеры 4. Поляризационные фильтры Верный ответ: 2	

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 обучающимися 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:

Курс лекций разбивается на три последовательных логических модуля:

1. Фундаментальный (лекции 1–5): Перевод понятий классической информатики на язык квантовой механики и линейной алгебры.
2. Алгоритмический / Криптоаналитический (лекции 6–12): Изучение квантовых схем, принципа работы базовых алгоритмов и механизмов взлома классических шифров (Шора, Гровера).
3. Защитный / Инженерный (лекции 13–18): Изучение квантовой коммуникации (QKD), постквантовых криптосистем и стандартов безопасности.

Типовая структура одной лекции (План подачи материала)

Каждое лекционное занятие (стандартные 2 академических часа / 90 минут) жестко структурировано для обеспечения максимальной scannability (читаемости) и усвояемости:

1. Вводная часть (5–10 минут)

Тема и план лекции: Озвучивание ключевых вопросов.

Связь с предыдущим материалом: Краткое повторение (например, перед разбором алгоритма Шора кратко повторяется квантовое преобразование Фурье).

Мотивационный блок: Объяснение, какую конкретную проблему информационной безопасности решает данная тема.

2. Теоретическое / Математическое обоснование (25–30 минут)

Введение математического аппарата (векторы, матрицы, операторы).

Формулировка физических ограничений или постулатов квантовой механики, применимых к теме.

Алгоритмическая / Схемотехническая часть (30 минут)

Построение квантовой схемы: Разбор вентилей, их последовательности и принципа трансформации квантовых состояний.

Пошаговая трассировка: Разбор работы алгоритма на простом примере (например, для 2-3 кубитов).

Криптографический анализ и применение (15 минут)

Оценка защищенности: Как данный алгоритм влияет на стойкость шифров (RSA, AES) или как протокол защищает от перехвата.

Ресурсный анализ: Сколько кубитов и времени требуется для реализации (теория vs реальная практика).

Заключительная часть (5 минут)

Резюме (Выводы): Краткая фиксация главных тезисов лекции.

Анонс: Связь с темой следующей лекции и лабораторной работы.

Форма и методическое обеспечение лекционного материала

Лекционный материал предоставляется студентам в мультимедийном и текстовом виде:

Презентационные материалы (Слайды): Основной визуальный якорь. Содержат минимум сплошного текста, акцент делается на квантовые схемы, архитектурные диаграммы сетей QKD и графики.

Конспект лекций (Скрипт): Текстовое пособие, включающее строгие математические выводы, которые тяжело воспринимать со слайдов.

Интерактивные демонстрации: Использование преподавателем в процессе лекции визуализаторов (например, среды *Quirk* или *IBM Quantum Composer*) для демонстрации «живого» изменения состояний кубитов на сфере Блоха.

11.2. Методические указания для обучающихся по прохождению практических занятий

Практическое занятие является одной из основных форм организации учебного процесса, заключающаяся в выполнении обучающимися под руководством преподавателя комплекса учебных заданий с целью усвоения научно-теоретических основ учебной дисциплины, приобретения умений и навыков, опыта творческой деятельности.

Целью практического занятия для обучающегося является привитие обучающимся умений и навыков практической деятельности по изучаемой дисциплине.

Планируемые результаты при освоении обучающимся практических занятий:

– закрепление, углубление, расширение и детализация знаний при решении конкретных задач;

– развитие познавательных способностей, самостоятельности мышления, творческой активности;

– овладение новыми методами и методиками изучения конкретной учебной дисциплины;

– выработка способности логического осмысления полученных знаний для выполнения заданий;

– обеспечение рационального сочетания коллективной и индивидуальной форм обучения.

Требования к проведению практических занятий

Требования к проведению практических занятий

1. Инфраструктурные и программные требования

- Техническое оснащение: наличие персонального компьютера с доступом в интернет для каждого студента. Квантовые вычисления моделируются локально или через облачные сервисы.
- Программная среда: предустановленный интерпретатор Python 3.10+ и среда разработки Jupyter Notebook или VS Code.
- Квантовые библиотеки: обязательное наличие актуальных версий библиотек Qiskit (IBM) или Cirq (Google) для написания кода.
- Облачный доступ: зарегистрированные учебные аккаунты на платформе IBM Quantum Platform для доступа к реальным квантовым процессорам (по возможности) и графическому конструктору Composer.
- Инструменты визуализации: доступ к веб-симулятору Quirk для быстрой прототипичной проверки схем без написания кода.

2. Методические требования к структуре занятия

Каждое практическое занятие длительностью 2 академических часа должно состоять из трех обязательных этапов:

Входной контроль и теория (15–20 минут): экспресс-опрос или аналитический разбор математической базы на доске. Студенты должны доказать понимание линейной алгебры (матриц, векторов, тензорных произведений) до начала работы на ПК.

Самостоятельное программирование (50–60 минут): выполнение практического задания по написанию квантового алгоритма или сборке схемы. Преподаватель выступает в роли ментора, помогая с отладкой квантовой логики.

Защита результатов (10–15 минут): демонстрация работающего кода, объяснение гистограмм распределения вероятностей или расчетных матриц плотности.

Требования к оформлению и результатам (KPI студента)

По итогам каждого занятия студент обязан предоставить отчет, содержащий:

Математический расчет: аналитический вывод формул, векторов состояний или матриц операторов, использованных в работе.

Файл кода: работающий скрипт в формате .ipynb (Jupyter) с подробными комментариями к каждому квантовому регистру и вентилю.

Графический анализ: скриншоты или графики (сфера Блоха, гистограммы измерений, схемы цепей) с интерпретацией полученных результатов.

Анализ ошибок: при моделировании шумов — расчет метрики Fidelity (верности состояния) до и после применения кодов коррекции.

Критерии оценивания

Практические работы оцениваются по многофакторной шкале:

Корректность математической модели: правильность аналитических вычислений и понимание постулатов (критерий: 30% оценки).

Работоспособность кода/схемы: отсутствие синтаксических и логических ошибок в квантовых цепях (критерий: 40% оценки).

Глубина анализа: умение объяснить, почему алгоритм дает именно такое распределение вероятностей при измерении (критерий: 20% оценки).

Защита работы: устные ответы на контрольные вопросы по теме занятия (критерий: 10% оценки).

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 обучающихсяявляются:

- 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.

Выполнение практических работ (40%): Разработка квантовых схем и программного кода, оформление и своевременная защита отчетов.

Контрольные работы / Тестирование (30%): Сдача промежуточных тестов по теории квантовой информатики и квантового криптоанализа.

Самостоятельная работа и активность на семинарах (20%): Решение практических задач у доски, разбор кейсов, подготовка докладов по современным стандартам постквантовой криптографии.

Посещаемость и ведение конспектов (10%): Регулярное присутствие на лекционных и практических занятиях.

Формы контроля и методические рекомендации по сдаче

Защита лабораторных работ

Сроки: Работа должна быть сдана в течение 1–2 недель после ее проведения по графику. За несвоевременную сдачу (без уважительной причины) рейтинг снижается на 20–50%.

Процедура: Студент демонстрирует преподавателю работающий код (в среде Qiskit/Jupyter) или схему, предоставляет отчет и устно отвечает на 2–3 контрольных вопроса.

Совет обучающемуся: Перед защитой повторите физический смысл используемых вентилей (например, зачем нужен вентиль Адамара в вашей схеме) и умейте объяснить каждую строчку своего кода.

Промежуточное тестирование (Текущие тесты)

Формат: Компьютерное или письменное тестирование по завершении крупных разделов (например, после Модуля 3 «Квантовый криптоанализ»).

Условия: Тест содержит 10–15 вопросов с ограничением по времени (в среднем 1.5–2 минуты на вопрос). Повторные попытки для повышения оценки обычно не предоставляются.

Совет обучающемуся: Обратите внимание на базовые понятия (свойства кубитов, отличия алгоритма Шора от Гровера, математические основы постквантовой криптографии). Тесты проверяют понимание сути процессов, а не заучивание сложных формул.

Контрольная работа (Решение задач)

Формат: Письменное решение практических задач (например, расчет выходного состояния квантовой схемы после прохождения вентилей Паули, или расчет уровня ошибок в протоколе BB84 при определенном типе атаки).

Совет обучающемуся: Тщательно расписывайте ход решения. Преподаватель оценивает логику рассуждений, даже если в финальном арифметическом расчете допущена ошибка.

Шкала оценивания и условия допуска к зачету

По итогам текущего контроля формируется семестровый рейтинг студента:

от 85 до 100 баллов — оценка «Отлично» (высокий уровень компетенций, возможен автоматический зачет).

от 71 до 84 баллов — оценка «Хорошо» (средний уровень, стабильная работа в семестре).

от 51 до 70 баллов — оценка «Удовлетворительно» (минимально допустимый уровень знаний).

менее 51 балла — оценка «Неудовлетворительно» (студент не освоил программу).

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».

Условия допуска к зачету

- Для получения допуска к промежуточной аттестации студент должен выполнить обязательный минимум учебной программы в семестре:
- Лабораторный практикум: Выполнить, оформить и успешно защитить все 5 лабораторных работ.

- Текущий контроль: Набрать по результатам текущего контроля успеваемости (балльно-рейтинговой системы) не менее 51 балла.
- При наличии академических задолженностей по лабораторным работам студент обязан ликвидировать их до начала зачетной сессии в дни консультаций преподавателя.

Формат и процедура проведения зачета

Зачет проводится в устно-письменной или тестовой форме по утвержденным вопросам (билетам):

1. Получение задания: Студент получает зачетный билет, который стандартно включает два теоретических вопроса (из разных разделов курса) и одно практическое задание (например, расчет состояния кубита после вентиля или анализ схемы).
2. Время на подготовку: На написание развернутого плана ответа и решение задачи студенту предоставляется 45 минут.
3. Использование материалов: Во время зачета категорически запрещено использование мобильных телефонов, шпаргалок, конспектов и сети Интернет. Допускается использование простой канцелярии.
4. Собеседование: Преподаватель выслушивает ответ студента по билету и может задать до 2–3 дополнительных или уточняющих вопросов в рамках программы дисциплины.

Критерии оценивания ответа студента

По результатам промежуточной аттестации выставляется бинарная оценка: «зачтено» или «не зачтено».

Оценка «Зачтено» выставляется, если студент:

Демонстрирует знание физико-математических основ квантовой информатики.

Понимает принципы работы алгоритмов Шора и Гровера, может объяснить характер их угроз для RSA, ECC и AES.

Свободно ориентируется в механизмах квантового распределения ключей (протоколы BB84, E91) и методах постквантовой защиты.

Успешно решил практическую задачу из билета или допустил в ней незначительную вычислительную ошибку, не нарушив логику квантовых преобразований.

Оценка «Не зачтено» выставляется, если студент:

Не может дать определения базовым понятиям (кубит, суперпозиция, квантовый вентиль).

Не понимает разницы между квантовым распределением ключей (физическая защита) и постквантовой криптографией (математическая защита).

Не справился с теоретическими вопросами билета и не смог ответить на наводящие вопросы преподавателя.

Нарушил правила проведения аттестации (использовал скрытые шпаргалки или технические средства).

Рекомендации по подготовке к зачету

Систематизация материала: Разделите вопросы к зачету на 4 смысловых блока (база, схемы, угрозы, защита) и повторяйте их последовательно.

Акцент на суть алгоритмов: Не зазубривайте сложные многомерные матрицы. Гораздо важнее понимать логику: какой вентиль создает суперпозицию (Адамар), какой связывает кубиты (CNOT), и почему алгоритм Шора работает быстрее классического перебора (за счет поиска периода функции через квантовое преобразование Фурье).

Повторение лабораторных: Просмотрите свои отчеты по лабораторным работам — практическая задача в билете часто дублирует элементы программного кода или расчетные таблицы из ваших работ.

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