МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)
ИНСТИТУТ НАУКОЕМКИХ ТЕХНОЛОГИЙ И ПЕРЕДОВЫХ МАТЕРИАЛОВ (ШКОЛА)

СОГЛАСОВАНО	УТВЕРЖДАЮ
Руководитель ОП ДТФИТ	И.о. зам. директора по учебной и воспитательной работе ИНТПМ
_____ Нефедев К.В.	_____ Красицкая С.Г.
(подпись) (ФИО)	(подпись) (ФИО.)
	«11» января 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность и квантовая криптография
Образовательная Программа уровня магистратуры
по направлению подготовки 03.04.02 Физика,
«Вычислительная физика и квантовые технологии»

Форма подготовки очная

курс 2 семестр 3
лекции не предусмотрены.
практические занятия 32 час.
лабораторные работы 32 час.
в том числе с использованием МАО 18 час.
всего часов аудиторной нагрузки 64 час.
самостоятельная работа 44 час.
в том числе на подготовку к экзамену не предусмотрено.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет 3 семестр
экзамен не предусмотрен

Рабочая программа составлена в соответствии с требованиями
Федерального государственного образовательного стандарта
по направлению подготовки **03.04.02 Физика,**
утвержденного приказом Министерства науки и высшего образования РФ
от 7 августа 2020 г. № 891.

Рабочая программа обсуждена на заседании Департамента теоретической физики и интеллектуальных технологий, протокол № 4 от «25» ноября 2021 г.
Директор Департамента: Нефедев К.В.
Составитель: профессор, д.ф.-м.н. Нефедев К.В.

Владивосток,
2022

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании ДТФИТ:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании ДТФИТ:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

III Рабочая программа пересмотрена на заседании ДТФИТ:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании ДТФИТ:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

1. Цели и задачи освоения дисциплины:

Дисциплина обеспечивает подготовку студентов в области методов фундаментальных знаний в новой области современных исследований - квантовой криптографии. Цели также включают в себя:

1) Освоение математического аппарата, используемого для задач квантовой криптографии.

2) Освоение принципов работы базовых квантовых криптографических протоколов распределения ключей.

3) Освоение принципов работы волоконно-оптических систем квантового распределения ключей, а также систем квантовой криптографии, работающих через открытое пространство.

4) Получение навыков разработки и доказательства криптографической стойкости систем квантовой криптографии.

5) Подготовка студентов к чтению современной научной литературы в данной области.

Профессиональные компетенции выпускников и индикаторы их достижения:

Тип задач	Код и наименование профессиональной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
Педагогический	**ПК-5** Способен осуществлять профессиональную деятельность в соответствии юридическими и морально-этическими нормами профессиональной этики	ПК-5.1 Применяет на практике требования законов и иных нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни)

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
ПК-5.1 Применяет на практике требования законов и иных нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни)	Знает требования законов и иных нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).
	Умеет использовать законы и иные нормативно-правовые документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).
	Владеет навыками использования нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).

Тип задач	Код и наименование профессиональной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
Педагогический	**ПК-5** Способен осуществлять профессиональную деятельность в соответствии юридическими и морально-этическими нормами профессиональной этики	ПК-5.2 Применяет в своей деятельности нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
ПК-5.2 Применяет в своей деятельности нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности	Знает нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности
	Умеет осуществлять деятельность с учетом норм профессиональной этики
	Владеет навыками обеспечения конфиденциальности сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности

2. Трудоёмкость дисциплины и видов учебных занятий по дисциплине

Общая трудоемкость дисциплины составляет 3 зачётные единицы (108 академических часов).

(1 зачетная единица соответствует 36 академическим часам)

Видами учебных занятий и работы обучающегося по дисциплине могут являться:

Обозначение	Виды учебных занятий и работы обучающегося
Лек	Лекции
Пр	Практические занятия
СР	Самостоятельная работа обучающегося в период теоретического обучения
Контроль	Самостоятельная работа обучающегося и контактная работа обучающегося с преподавателем в период промежуточной аттестации

Структура дисциплины:

Форма обучения – очная.

№	Наименование Практическая работаа дисциплины	Семестр	Количество часов по видам учебных занятий и работы обучающегося						Формы промежуточной аттестации
			Лек	Пр	Лаб	ОК	СР	Контроль	
1	Практическая работа 1. Методы практической чистки первичных ключей и методы сжатия (хэширования – усиления секретности) ключей в квантовой криптографии. Методы коррекции ошибок основанные на классических кодах корректирующих ошибки. Итерационные адаптивные процедуры исправления ошибок.	3		3	3	-	38	-	ПК-5.1; ПК-5.2;
2	Практическая работа 2. Анализ стойкости реализаций систем квантовой криптографии с не идеальными источниками квантовых состояний, детекторами и квантовым каналом связи с потерями. Атака с расщеплением по числу фотонов. Атака с подменой фазы в системах с фазовым кодированием. Атака с ослеплением фотодетекторов.			3	3				ПК-5.1; ПК-5.2;
3	Практическая работа 3. Протоколы устойчивые по отношению к атаке с ослеплением фотодетекторов. Побочные каналы утечки информации в системах квантовой криптографии, фундаментальная квантово - механическая верхняя граница на утечку информации по побочным каналам.			3	3				ПК-5.1; ПК-5.2;
4	Практическая работа 4. Основы математического аппарата для анализа стойкости систем квантовой криптографии с конечными длинами передаваемых последовательностей. Критерий составной секретности ключей, основанный на следовом расстоянии.			3	3				ПК-5.1; ПК-5.2;
5	Практическая работа 5. Основные свойства квантовых			3	3				ПК-5.1; ПК-5.2;

	энтропий Реньи (min и max энтропий). Сглаженные min и max энтропии, цепочечные правила, изменение min и max энтропий при действии супероператора, свойства min и max энтропии для составных квантовых систем.								
6	Практическая работа 6. Теорем s de Finetti классический и квантовые случаи. Min и max энтропий для тензорного произведения матриц плотности. Симметричные состояния. Min и max энтропий для симметричных состояний. Необходимые неравенства для различных расстояний между квантовыми состояниями.			3	3				ПК-5.1; ПК-5.2;
7	Практическая работа 7. Коррекция ошибок с минимальной утечкой информации при помощи универсальных хэш -функций второго порядка.			3	3				ПК-5.1; ПК-5.2;
8	Практическая работа 8. Квантовое усиление секретности. Квантовая теорема усиления секретности – теорема об остатке хэширования. Примеры доказательств секретности BB84 и фазово - временной квантовой криптографии с использованием аппарата квантовых min и max энтропий (асимптотический предел).			3	3				ПК-5.1; ПК-5.2;
9	Практическая работа 9. Энтропийные соотношения неопределенностей в квантовой криптографии. Связь с min и max энтропиями.			3	3				ПК-5.1; ПК-5.2;
10	Практическая работа 10. Анализ стойкости квантового протокола распределения ключей BB84 с конечными передаваемыми последовательностями (доказательство с использованием энтропийных соотношений неопределенности).			3	3				ПК-5.1; ПК-5.2;
11	Практическая работа 11. Доказательства стойкости фазово-временной и релятивистской квантовой криптографии для открытого пространства с			2	2				ПК-5.1; ПК-5.2;

	конечными длинами последовательностей с использованием аппарата квантовых min и max энтропий.								
10	Итого:	3	-	32	32	-	38	-	

3. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Лекционные занятия

Не предусмотрены.

4. СТРУКТУРА И СОДЕРЖАНИЕ ЛАБОРАТОРНЫХ РАБОТ

Лабораторные работы

Лабораторная 1 Простейший алгоритм квантовой генерации ключа
Лабораторная 2 Алгоритм Беннета
Лабораторная 3 Квантовый криптоанализ
Лабораторная 4 Квантовые системы шифрования
Лабораторная 5 Постквантовые криптографические алгоритмы
Лабораторная 6 Применение квантовых кодов коррекции ошибок

5. СТУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа 1. Методы практической чистки первичных ключей и методы сжатия (хэширования – усиления секретности) ключей в квантовой криптографии. Методы коррекции ошибок основанные на классических кодах корректирующих ошибки. Итерационные адаптивные процедуры исправления ошибок.
Практическая работа 2. Анализ стойкости реализаций систем квантовой криптографии с не идеальными источниками квантовых состояний, детекторами и квантовым каналом связи с потерями. Атака с расщеплением по числу фотонов. Атака с подменой фазы в системах с фазовым кодированием. Атака с ослеплением фотодетекторов.
Практическая работа 3. Протоколы устойчивые по отношению к атаке с ослеплением фотодетекторов. Побочные каналы утечки информации в системах квантовой криптографии, фундаментальная квантово - механическая верхняя граница на утечку информации по побочным каналам.
Практическая работа 4. Основы математического аппарата для анализа стойкости систем квантовой криптографии с конечными длинами передаваемых последовательностей. Критерий составной секретности ключей, основанный на следовом расстоянии.
Практическая работа 5. Основные свойства квантовых энтропий Реньи (min и max энтропий). Сглаженные min и max энтропии, цепочечные правила, изменение min и max энтропий при действии супероператора, свойства min и max энтропии для составных квантовых систем.

Практическая работа 6. Теорем s de Finetti классический и квантовые случаи. Min и max энтропий для тензорного произведения матриц плотности. Симметричные состояния. Min и max энтропий для симметричных состояний. Необходимые неравенства для различных расстояний между квантовыми состояниями.
Практическая работа 7. Коррекция ошибок с минимальной утечкой информации при помощи универсальных хэш -функций второго порядка.
Практическая работа 8. Квантовое усиление секретности. Квантовая теорема усиления секретности – теорема об остатке хэширования. Примеры доказательств секретности BB84 и фазово - временной квантовой криптографии с использованием аппарата квантовых min и max энтропий (асимптотический предел).
Практическая работа 9. Энтропийные соотношения неопределенностей в квантовой криптографии. Связь с min и max энтропиями.
Практическая работа 10. Анализ стойкости квантового протокола распределения ключей BB84 с конечными передаваемыми последовательностями (доказательство с использованием энтропийных соотношений неопределенности).
Практическая работа 11. Доказательства стойкости фазово-временной и релятивистской квантовой криптографии для открытого пространства с конечными длинами последовательностей с использованием аппарата квантовых min и max энтропий.

5. СТРУКТУРА, СОДЕРЖАНИЕ, УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине включает в себя:

- план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;
- требования к представлению и оформлению результатов самостоятельной работы;
- критерии оценки выполнения самостоятельной работы.

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Вид самостоятельной работы	Дата/сроки выполнения	Примерные нормы времени на выполнение	Форма контроля
1	1-3 недели семестра	Подготовка к лабораторным работам	10 час.	УК-1.2 собеседование; ПК-1.3 конспект
2	4-6 недели семестра	Подготовка к лабораторным работам	9 час.	УК-1.2 собеседование; ПК-1.3 конспект
3	7-8 недели семестра	Подготовка к лабораторным работам	10 час.	УК-1.2 собеседование; ПК-1.3 конспект

4	9-10 недели семестра	Подготовка к лабораторным работам	9 час.	УК-1.2 собеседование; ПК-1.3 конспект
4	11-13 недели семестра	Подготовка к лабораторным работам	10 час.	УК-1.2 собеседование; ПК-1.3 конспект
5	14-15 недели семестра	Подготовка к лабораторным работам	10 час.	УК-1.2 собеседование; ПК-1.3 конспект
6	16-18 недели семестра	Подготовка к лабораторным работам	10 час.	УК-1.2 собеседование; ПК-1.3 конспект
Итого:			58 час.	

Рекомендации по самостоятельной работе студентов

Планирование и организация времени, отведенного на выполнение заданий самостоятельной работы.

Изучив график выполнения самостоятельных работ, следует правильно её организовать. Рекомендуется изучить конспект лекционного материала, соответствующий теме каждого практического занятия и, при необходимости, рассмотреть и детализировать отдельные интересующие или вызывающие затруднения в понимании моменты с помощью рекомендуемой литературы. Отчетность по каждому заданию предоставляется в последнюю неделю согласно графику.

Требования к представлению и оформлению результатов самостоятельной работы

При подготовке к устному опросу (УК-1.2) воспользоваться материалами из рекомендованной литературы. Оцениваются:

- владение материалом;
- умение формулировать свои мысли, отстаивать свою точку зрения;
- умение задавать вопросы оппоненту;
- умение отвечать на вопросы оппонента;
- умение подвести итого по результатам обсуждения.

Контроль результатов самостоятельной работы студентов осуществляется в пределах времени, отведенного на обязательные учебные занятия и внеаудиторную самостоятельную работу студентов по дисциплине, проводится в письменной и устной форме.

Контроль самостоятельной работы студентов предусматривает:

- соотнесение содержания контроля с целями обучения;
- объективность контроля;
- валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить).

Критерии оценки результатов самостоятельной работы

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентов учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность общеучебных умений;
- умения студента активно использовать электронные образовательные ресурсы, находить требующуюся информацию, применять на практике;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;
- умение ориентироваться в потоке информации, выделять главное;
- умение сформировать свою позицию, оценку и аргументировать ее.

6. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые Практическая работаы / темы дисциплины	Код и наименование индикатора достижения компетенции	Результаты обучения	Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Практическая работаы 1-2	ПК-5.1 Применяет на практике требования законов и иных нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни)	Знает требования законов и иных нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).	Отчет	Зачёт (вопросы)
			Умеет использовать законы и иные нормативно-правовые документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).		
			Владеет навыками использования нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).		
	Практическая работаы 3-4	ПК-5.2 Применяет в своей деятельности нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности	Знает нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности	Отчет	Зачёт (вопросы)
			Умеет осуществлять деятельность с учетом норм профессиональной этики		
			Владеет навыками обеспечения конфиденциальности сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности		
	Практическая работаы 5-6	ПК-5.2 Применяет в своей деятельности нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных	Знает нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности	Отчет	Зачёт (вопросы)
			Умеет осуществлять деятельность с учетом норм профессиональной этики		

		отношений, полученных в процессе профессиональной деятельности	Владеет навыками обеспечения конфиденциальности сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности		

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие результаты обучения, представлены в Приложении

7. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. А.С.Холево. Квантовые системы, каналы, информация, Москва. МЦМО, сс.327 (2010); S. Holevo, Introduction to Quantum Information

Theory, (MTNMO, Moscow, 2002) [in Russian]; Usp. Mat. Nauk, 53, 193 (1998); А.С.Холево, Информационная безопасность и квантовая криптография, серия Современная математическая физика, вып.5}, МЦНМО, Москва, 2002

2. М.Нильсен, И.Чанг, Квантовые вычисления и информация, изд. Мир, Москва, (2006).

3. Дж. Прескилл, Квантовая информация и квантовые вычисления, том 1, изд. R&C Dynamics, Ижевск, (2008).

4. C.E.Shannon, Mathematical Theory of Communication, Bell Syst. Tech. Jour., 27, 397; 27, 623 (1948).

5. Р.Галлагер, Теория информации и надежная связь, (Советское радио, 1974);

6. R. G. Gallager, Information Theory and Reliable Communication, (Wiley, New York, 1968)

Дополнительная литература

(печатные и электронные издания)

1. W.K.Wootters, W.H.Zurek, A single quantum cannot be cloned, Nature, {299, 802 (1982).

2. C.H.Bennett, G.Brassard, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, 175 (1984).

3. C.H.Bennett, Phys. Rev. Lett., 68, 3121 (1992).

4. R.Renner, Security of Quantum Key Distribution, PhD Thesis, ETH Z\"urich, Dec. 2005. arXiv/quant-ph: 0512258.

5. V.Scarani, H.Bechmann-Pasquinucci, N.J.Cerf, M.Dusek, N.Lutkenhaus,

6. M.Peev, Rev. Mod. Phys., 81, 1301 (2009).

7. D.Mayers, Journal ACM, 48 351 (2001).

8. H.-K.Lo, H.F.Chau, Science, 283 2050 (1999).

9. P.Shor, J.Preskill, Phys. Rev. Lett., 85 441 (2000).

10. M.Koashi, J. Phys. Conf. Ser., 36, 98 (2006).

11. M.Tomamichel. R.Renner, The Uncertainty Relation for Smooth Entropies, arXiv/quant-ph: 10092015.

12. M.Tomamichel, C.Ci Wen Lim, N.Gisin, R.Renner, Tight Finite-Key Analysis for Quantum Cryptography, arXiv/quant-ph: 11034130.

13. С.П.Кулик, А.П.Маккавеев, С.Н.Молотков, Письма в ЖЭТФ. 85, 354 (2007).

14. С.Н.Молотков, ЖЭТФ. 133, 5 (2008).

15. Д.А.Кронберг, С.Н.Молотков, ЖЭТФ, 136, 650 (2009); ЖЭТФ, 138, 33 (2010).

16. H.P.Robertson, Phys. Rev., 34, 163 (1929).

17. D.Deutsch, Phys. Rev. Lett., 50, 631 (1983).

18. K.Kraus, Phys. Rev., D 35, 3070 (1987).

19. H.Maassen, J.B.M.Uffink, Phys. Rev. Lett., {\bf 60}, 1103 (1988).

20. J.M.Renes, J.-C. Boileau, Phys. Rev. Lett., 103, 020402-1 (2009).

21. M.Berta, M.Chritlandl, R.Colbeck, J.M.Renes, R.Renner, The Uncertainty Principle in the Presence of Quantum Memory, arXiv/quant-ph: 0909.0950.

22. M.Cover J.A.Thomas. Elements of Information Theory. Wiley, (1991).

23. M.Berta, M.Christandl, R.Colbeck, J.M.Renes, R.Renner, Nature Physics, 6, 659 (2010).

24. M.Tomamichel, R.Renner, The Uncertainty Relation for Smooth Entropies, arXiv/quant-ph: 10092015.

25. J.M.Renes, R.Renner, One-Shot Classical Data Compression withQuantum Side Information and the Distillation of Common Randomness or Secret Keys,

arXiv/quant-ph: 10080452.

26. J.L.Carter, M.N.Wegman Universal Classes of Hash Functions, J. Comp. Syst. Sci., 18, (1979) 143.

27. M.N.Wegman, J.L.Carter, New Hash Functions and Their Use Authentication and Set Euqality, J. Comp. Syst. Sci., 22, 265 (1991).

28. C.H.Bennett, G.Brassard, C.Crepeau, U.M.Maurer, Generalized Privacy Amplication, IEEE Trans. on Inf. Theory, 41 (1995) 1915.

29. M.Tomamichel, C.Schaffner, A.Smith, R.Renner, Leftover Hashing Against Quantum Side Information, arXiv/quant-ph: 10022436.

30. D.R.Stinson, On the Connections Between Universal Hashing, Combinatorial Designs and Error-Correcting Codes, ECCC TR95-052, Electronic

Colloquium on Computational Complexity - Reports Series (1995).

31. W.Hoeffding, Probability Inequalities for Sums of Bounded Random Variables, J. Amer. Statistical Assoc., 58 (1963) 13.

32. R. J. Serfling, Probability Inequalities for the Sum in Sampling without Replacement ,Ann. Stat., 2 (1974) 39.

33. L.Lydersen, C.Wiechers, C.Wittmann, D.Elser, J.Skaar, V.Makarov,

34. Hacking commercial quantum cryptography systems by tailored bright illumination, Nature Photonics, 4, 686 (2010).

35. С.Н.Молот ков, "Энтропийные соотношения неопределенностей и стойкость фазово-временной квантовой криптографии при конечных длинах передаваемых последовательностей" Журнал экспериментальной и теоретической физики, т. 142 (2012) 1-19.

36. С.Н.Молотков, "О стойкости релятивистской квантовой криптографии в открытом пространстве при конечных ресурсах".Письма в журнал экспериментальной и теоретической физики, т. 96 (2012) 374.

37. С.П.Кулик, С.Н.Молотков, И.В.Радченко, "О квантовом распределении ключей на композитных фотонах -- поляризационных кутритах." Письма в журнал экспериментальной и теоретической физики, т. 96 (2012) 367.

38. С.Н.Молотоков, "О геометрически однородных когерентных состояниях в квантовой криптографии", Письма в журнал экспериментальной и теоретической физики, т. 95 (2012) 361.

39. С.Н.Молотков, "Об уязвимости базовых протоколов квантового распределения ключей и о трех протоколах, устойчивых к атаке с "ослеплением" лавинных детекторов", Журнал экспериментальной и теоретической физики, т. 141 (2012) 812-831.

40. С.Н.Молотков,"О решении проблемы обеспечения стойкости квантовой криптографии для канала связи со сколь угодно большой длиной", Письма в журнал экспериментальной и теоретической физики, т. 93 (2011) 830.

41. С.Н.Молотков,"Квантовое распределение ключей без передачи квантового состояния как целого через канал связи", Письма в журнал экспериментальной и теоретической физики, т. 93 (2011) 389.

42. С.Н.Молотков, "Релятивистская квантовая криптография для открытого пространства без синхронизации часов на передающей и приемной стороне", Письма в журнал экспериментальной и теоретической физики, т. 94 (2011) 504.

43. С.Н.Молотков, "Энтропийные соотношения неопределенностей и предельно допустимая критическая ошибка в квантовой криптографии". Письма в журнал экспериментальной и теоретической физики, т. 94 (2011) 900.

44. Молотков, "Квантовое распределение ключей с эталонным квантовым состоянием", Журнал экспериментальной и теоретической физики, т. 140 (2011) 857.

45. С.Н.Молотков, Релятивистская квантовая криптография, Журнал экспериментальной и теоретической физики, т. 139 (2011) 139.

46. Д.А.Кронберг, С.Н.Молотков, Усиление стойкости фазово-временной квантовой криптографии блочным исправлением ошибок,, Письма в
ЖЭТФ, т.92, (2010) 539.
47. Д.А.Кронберг, С.Н.Молотков, Квантовая схема для оптимального подслушивания фазово-временной квантовой криптографии ,ЖЭТФ, т.138
(2010) 33.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Основной Интернет-ресурс по квантовой информатике и квантовой криптографии: международный архив электронных препринтов Корнельского университета: xxx.lanl.gov\quant-ph

2. http://www.aps.org – журналы Американского физического общества,

3. jetpletters.ac.ru, jetp.ac.ru – журналы Российской академии наук.

1.

2. Перечень информационных технологий и программного обеспечения

При осуществлении образовательного процесса по дисциплине используется общее программное обеспечение компьютерных учебных классов (Windows XP, Microsoft Office и др.).

8.МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Планирование и организация времени, отведенного на изучение дисциплины. Приступить к освоению дисциплины следует незамедлительно в самом начале учебного семестра. Рекомендуется изучить структуру и основные положения Рабочей программы дисциплины. Обратить внимание, что кроме аудиторной работы (лекции, практические занятия) планируется самостоятельная работа, итоги которой влияют на окончательную оценку по итогам освоения учебной дисциплины. Все задания (аудиторные и самостоятельные) необходимо выполнять и предоставлять на оценку в соответствии с графиком.

В процессе изучения материалов учебного курса предлагаются следующие формы работ: чтение лекций, практические занятия.

Лекционные занятия ориентированы на освещение вводных тем в каждый Практическая работа курса и призваны ориентировать студентов в предлагаемом материале, заложить теоретические и методологические основы для дальнейшей самостоятельной работы студентов.

Лабораторные работы акцентированы на принципиальных вопросах курса и призваны стимулировать выработку практических умений.

При подготовке к практическому занятию необходимо сначала ознакомиться с материалом лекции, а затем с материалами из основной и дополнительной литературы. Выучить основной теоретический материал по теме (по материалам лекций и основной литературы).

При работе с литературой необходимо внимательно изучать Практическая работаы, соответствующие теме занятия, при поиске информации в электронных системах необходимо правильно сформулировать поисковый запрос, лучше использовать несколько вариантов запроса для расширения возможности поиска информации в сети интернет. Использовать можно только информацию с официальных тематических сайтов или сайтов организаций.

Особо значимой для профессиональной подготовки студентов является *самостоятельная работа* по курсу. В ходе этой работы студенты отбирают необходимый материал по изучаемому вопросу и анализируют его. Студентам необходимо ознакомиться с основными источниками, без которых невозможно полноценное понимание проблематики курса.

Освоение курса способствует развитию навыков обоснованных и самостоятельных оценок фактов и концепций. Поэтому во всех формах контроля знаний, особенно при сдаче зачета, внимание обращается на понимание проблематики курса, на умение практически применять знания и делать выводы.

Работа с литературой. Рекомендуется использовать различные возможности работы с литературой: фонды научной библиотеки ДВФУ и электронные библиотеки (http://www.dvfu.ru/library/), а также доступные для использования другие научно-библиотечные системы.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебные занятия по дисциплине могут проводиться в следующих помещениях, оснащенных соответствующим оборудованием и программным обеспечением, расположенных по адресу 690022, г. Владивосток, о.Русский, п. Аякс, 10:

Перечень материально-технического и программного обеспечения дисциплины приведен в таблице.

Наименование специальных помещений и помещений для самостоятельной работы[1]	Оснащенность специальных помещений и помещений для проведения учебных занятий, для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Учебные аудитории для проведения учебных занятий:		

1 В соответствии с п.4.3. ФГОС

690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус L, ауд. L 561а. Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 30). Доска аудиторная.	Специализированное ПО не требуется
Помещения для самостоятельной работы:		
А1042 аудитория для самостоятельной работы студентов	Моноблок Lenovo C360G-i34164G500UDK – 115 шт.; Интегрированный сенсорный дисплей Polymedia FlipBox; Копир-принтер-цветной сканер в e-mail с 4 лотками Xerox WorkCentre 5330 (WC5330C; Полноцветный копир-принтер-сканер Xerox WorkCentre 7530 (WC7530CPS Оборудование для инвалидов и лиц с ограниченными возможностями здоровья: Дисплей Брайля Focus-40 Blue – 3 шт.; Дисплей Брайля Focus-80 Blue; Рабочая станция Lenovo ThinkCentre E73z – 3 шт.; Видео увеличитель ONYX Swing-Arm PC edition; Маркер-диктофон Touch Memo цифровой; Устройство портативное для чтения плоскопечатных текстов PEarl; Сканирующая и читающая машина для незрячих и слабовидящих пользователей SARA; Принтер Брайля Emprint SpotDot - 2 шт.; Принтер Брайля Everest - D V4; Видео увеличитель ONYX Swing-Arm PC edition; Видео увеличитель Topaz 24” XL стационарный электронный; Обучающая система для детей тактильно-речевая, либо для людей с ограниченными возможностями здоровья; Увеличитель ручной видео RUBY портативный – 2 шт.; Экран Samsung S23C200B; Маркер-диктофон Touch Memo цифровой.	Microsoft Windows 7 Pro MAGic 12.0 Pro, Jaws for Windows 15.0 Pro, Open book 9.0, Duxbury BrailleTranslator, Dolphin Guide (контракт № А238-14/2); Неисключительные права на использование ПО Microsoft рабочих станций пользователей (контракт ЭА-261-18 от 02.08.2018): - лицензия на клиентскую операционную систему; - лицензия на пакет офисных продуктов для работы с документами включая формат.docx , .xlsx , .vsd , .ptt.; - лицензия па право подключения пользователя к серверным операционным системам , используемым в ДВФУ : Microsoft Windows Server 2008/2012; - лицензия на право подключения к серверу Microsoft Exchange Server Enterprise; - лицензия па право подключения к внутренней информационной системе документооборота и порталу с возможностью поиска информации во множестве удаленных и локальных хранилищах, ресурсах, библиотеках информации, включая портальные хранилища, используемой в ДВФУ: Microsoft SharePoint; - лицензия на право подключения к системе централизованного управления рабочими станциями, используемой в ДВФУ: Microsoft System Center.

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Фонды оценочных средств представлены в приложении.

(фонды оценочных средств включают в себя: перечень форм оценивания, применяемых на различных этапах формирования компетенций в ходе освоения дисциплины модуля, шкалу оценивания каждой формы, с описанием индикаторов достижения освоения дисциплины согласно заявленных компетенций, примеры заданий текущего и промежуточного контроля, заключение работодателя на ФОС (ОМ))

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

НАЗВАНИЕ ШКОЛЫ (ФИЛИАЛА)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
Информационная безопасность и квантовая криптография
Образовательная Программа уровня магистратуры по направлению подготовки 03.04.02 Физика, «Вычислительная физика и квантовые технологии», совместно с МФТИ

Форма подготовки очная

Владивосток
2021

Перечень форм оценивания, применяемых на различных этапах формирования компетенций в ходе освоения дисциплины / модуля

№ п/п	Контролируемые Практическая работаы / темы дисциплины	Код и наименование индикатора достижения компетенции	Результаты обучения	Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Практическая работаы 1-2	ПК-5.1 Применяет на практике требования законов и иных нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни)	Знает требования законов и иных нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).	Отчет	Зачёт (вопросы)
			Умеет использовать законы и иные нормативно-правовые документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).		
			Владеет навыками использования нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).		
	Практическая работаы 3-4	ПК-5.2 Применяет в своей деятельности нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности	Знает нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности	Отчет	Зачёт (вопросы)
			Умеет осуществлять деятельность с учетом норм профессиональной этики		
			Владеет навыками обеспечения конфиденциальности сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности		
	Практическая работаы 5-6	ПК-5.2 Применяет в своей деятельности нормы профессиональной этики, обеспечивает	Знает нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности	Отчет	Зачёт (вопросы)

		конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности	Умеет осуществлять деятельность с учетом норм профессиональной этики		
			Владеет навыками обеспечения конфиденциальности сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности		

Оценочные средства для текущего контроля

Текущая аттестация студентов по дисциплине проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация проводится в форме контрольных мероприятий по оцениванию фактических результатов обучения студентов и осуществляется ведущим преподавателем.

Объектами оценивания выступают:

− учебная дисциплина (своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);

− степень усвоения теоретических знаний;

− уровень овладения практическими умениями и навыками по всем видам учебной работы;

− посещение занятий

− результаты самостоятельной работы.

Составляется календарный план контрольных мероприятий по дисциплине. Оценка посещаемости, своевременность выполнения различных видов заданий ведётся на основе журнала, который ведёт преподаватель в течение учебного семестра.

Вопросы для собеседования

1. Информационная безопасность и квантовая криптография

2 Протокол BB84

3 Имитация работы протокола BB84

4 Протокол B92

5 Зацепленные состояния, неравенства Белла и протокол E91.

6 Протокол Lo05

7 Аппаратное обеспечение для квантовой криптографии.

Оценка	**Описание схемы оценивания**
«Отлично»	Показывает глубокое и прочное усвоение материала Практическая работаа. Полные, последовательные, грамотные и логически излагаемые ответы. Демонстрация обучающимся знаний в объеме рекомендованной и дополнительной литературы. Учебный материал воспроизводится с требуемой степенью точности.
«Хорошо»	Наличие в ответе несущественных ошибок, уверенно исправляемых после дополнительных и наводящих вопросов. Демонстрация обучающимся знаний в объеме пройденной программы; чёткое изложение изученного материала.
«Удовлетворительно»	Наличие несущественных ошибок в ответе, не исправляемых обучающимся. Демонстрация недостаточно полных знаний по пройденной программе, неструктурированное, нестройное изложение учебного материала при ответе.
«Неудовлетворительно»	Демонстрирует непонимание проблемы, незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

Оценочные средства для промежуточной аттестации

Код и наименование индикатора достижения компетенции	Результаты обучения	Шкала оценивания промежуточной аттестации			
		Неудовлетворительно	**Удовлетворительно**	**Хорошо**	**Отлично**
ПК-5.1 Применяет на практике требования законов и иных нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни)	Знает требования законов и иных нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).	*Не знает* требования законов и иных нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).	*Знает* требования законов и иных нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни), *но при этом допущены 1-2 существенные ошибки.*	*Знает требования законов и иных нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни), но допущены 2-3 несущественные ошибки.*	*Знает* требования законов и иных нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).
	Умеет использовать законы и иные нормативно-правовые документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).	*Не может* использовать законы и иные нормативно-правовые документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).	*Умеет использовать законы и иные нормативно-правовые документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни), но при этом допущены*	*Умеет использовать законы и иные нормативно-правовые документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни), но допущены 2-3*	*Умеет* использовать законы и иные нормативно-правовые документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).

			1-2 существенные ошибки.	*несущественные ошибки.*	
	Владеет навыками использования нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).	*Не владеет навыками использования нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).*	*Владеет навыками использования нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни)., но при этом допущены 1-2 существенные ошибки.*	*Владеет навыками использования нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни)., но допущены 2-3 несущественные ошибки.*	*Владеет* навыками использования нормативно-правовых документов в сфере образования (в т.ч., содержащие санитарно-гигиенические требования к образовательному процессу и нормы безопасности жизни).

Код и наименование индикатора достижения компетенции	**Результаты обучения**	**Шкала оценивания промежуточной аттестации**			
		Неудовлетворительно	**Удовлетворительно**	**Хорошо**	**Отлично**
ПК-5.2 Применяет в своей деятельности нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности	Знает нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности	*Не знает нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности*	*Знает нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности, но при этом допущены 1-2 существенные ошибки.*	*Знает нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности, но допущены 2-3 несущественные ошибки.*	*Знает* нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности

	Умеет осуществлять деятельность с учетом норм профессиональной этики	*Не может осуществлять деятельность с учетом норм профессиональной этики*	*Умеет осуществлять деятельность с учетом норм профессиональной этики, но при этом допущены 1-2 существенные ошибки.*	*Умеет осуществлять деятельность с учетом норм профессиональной этики, но допущены 2-3 несущественные ошибки.*	*Умеет осуществлять деятельность с учетом норм профессиональной этики*
	Владеет навыками обеспечения конфиденциальности сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности	*Не владеет навыками обеспечения конфиденциальности сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности*	*Владеет навыками обеспечения конфиденциальности сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности, но при этом допущены 1-2 существенные ошибки.*	*Владеет навыками обеспечения конфиденциальности сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности, но допущены 2-3 несущественные ошибки.*	*Владеет навыками обеспечения конфиденциальности сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности*

Вопросы к зачёту

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерный перечень вопросов и заданий

Реферат
Тематика рефератов

1. Классические шифры.
2. Применение шифра гаммирования.
3. Законы распределения вероятности.
4. Методы получения случайных двоичных последовательностей.
5. Критерий Шеннона абсолютной секретности.
6. Протокол квантовой телепортации.
7. Протокол BB84.
8. Протокол B92.
9. Протокол E91.
10. Протокол SARG04.
11. Фазово-временное кодирование информации в системах связи.
12. Дифференциально-фазовое кодирование информации.
13. Основы математического аппарата классической теории и информации.
14. Энтропии Шеннона, Реньи и их свойства.
15. Оптические элементы квантово-криптографических систем.

Зачетно-экзаменационные материалы для промежуточной аттестации (экзамен)

1. История криптографии.
2. Шифры гаммирования.
3. Что такое квантовая криптография, и какие задачи она решает.
4. Одноразовые ключи.
5. Существующие достижения в квантовой криптографии.
6. Основы математического аппарата квантовой информатики.
7. Описание квантовых состояний отдельных и составных квантовых систем.

8. Смешанные состояния, квантовая запутанность.
9. Ортогональные и обобщенные измерения.
10. Очищение квантовых состояний.
11. Теорема о запрете копирования, преобразования квантовых систем.
12. Меры близости квантовых состояний, используемые в протоколах квантовой криптографии.
13. Теорема о невозможности копирования и протокол квантовой телепортации.
14. Основные протоколы квантового распределения ключей.
15. Когерентные состояния и их преобразования оптическими элементами.
16. Волоконные реализации систем квантовой криптографии.
17. Неформальное введение в классическую теорию информации.
18. Релятивистское квантовое распределение ключей через открытое пространство с синхронизацией и без синхронизации часов на приемной и передающей стороне.