Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение

высшего образования «Новосибирский национальный исследовательский государственный университет» (Новосибирский государственный университет, НГУ)

Высший колледж информатики

Согласовано

Директор ВКИ НГУ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.Г. Окунев

*подпись*

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

***Шифрование и квантовая информатика***

направление подготовки: *15.03.06 Мехатроника и робототехника*

направленность (профиль): *Мехатроника и робототехника*

Форма обучения: очная

Разработчики:

Ассистент Е. А. Якшина

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель программы:

д.т. н., Назаров А.Д. . \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Новосибирск, 2020

**Содержание**

[**Содержание** 2](#_Toc59439825)

[1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы 3](#_Toc59439826)

[2. Место дисциплины в структуре образовательной программы 4](#_Toc59439827)

[3. Трудоемкость дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося 4](#_Toc59439828)

[4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий 4](#_Toc59439829)

[5. Перечень учебной литературы 6](#_Toc59439830)

[6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины 6](#_Toc59439831)

[7. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине 6](#_Toc59439832)

[8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине 7](#_Toc59439833)

[9. Оценочные средства для проведения текущего контроля и промежуточной аттестации по дисциплине 7](#_Toc59439834)

Приложение 1 Аннотация по дисциплине

Приложение 2 Оценочные средства по дисциплине

# 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

| Результаты освоения образовательной программы  (компетенции) | В результате изучения дисциплины обучающиеся должны: | | |
| --- | --- | --- | --- |
| знать | уметь | владеть |
| ОПК-2 Владение физико-математическим аппаратом, необходимым для описания мехатронных и робототехнических систем. | основные направления развития мехатроники и робототехники | применять физико-математический аппарат и рассчитывать матмодели устройств |  |
| ОПК-6 Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. | как использовать информационно-коммуникационные технологии при поиске необходимой информации, современные принципы и методы поиска, хранения, обработки, анализа и представления в требуемом формате информации |  | навыками получения, хранения переработки информации и обеспечения информационной безопасности |
| ПК-3 Способность разрабатывать экспериментальные макеты управляющих, информационных и исполнительных модулей мехатронных и робототехнических систем и проводить их экспериментальное исследование с применением современных информационных технологий. | основные методы разработки экспериментальных макетов управляющих, информационных и исполнительных модулей мехатронных и робототехнических систем |  |  |

# 2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), изучение которых необходимо для освоения дисциплины Шифрование и квантовая информатика:

помимо базовых физических принципов и понятий из курса «Механика» также требуются знания, изученные в курсе «Электродинамика» (в особенности особенно раздел про электромагнитные волны). Навыки построения алгоритмов как для шифрования так и для квантовых вычислений задаются в курсах «Модели вычислений» и «Методы оптимизации».

Дисциплины (практики), для изучения которых необходимо освоение дисциплины Шифрование и квантовая информатика:

# 3. Трудоемкость дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося

Трудоемкость дисциплины – 3 з.е. (108 ч)

Форма промежуточной аттестации: дифференцированный зачёт

|  |  |  |
| --- | --- | --- |
| № | Вид деятельности | Семестр |
| 7 |
| 1 | Лекции, ч | 32 |
| 2 | Практические занятия, ч | 0 |
| 3 | Лабораторные работы, ч | 32 |
| 4 | Занятия в контактной форме, ч, из них | 66 |
| 5 | из них аудиторных занятий, ч | 64 |
| 6 | в электронной форме, ч | - |
| 7 | консультаций, час. | - |
| 8 | промежуточная аттестация, ч | 2 |
| 9 | Самостоятельная работа, час. | 42 |
| 10 | Всего, ч | 108 |

# 4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Лекции (32 ч)

|  |  |
| --- | --- |
| Наименование темы и их содержание | Объем,  час |
| Раздел 1 Квантовая криптография | |
| 1. История шифрования. От простейших способов до современных алгоритмов. Симметричные криптосистемы, системы с открытым ключом. | 2 |
| 2. Различие между традиционной и квантовой криптографией. Физические принципы, лежащие в основе квантовой криптографии. | 2 |
| 3. Фотон, поляризация фотона. Квант энергии. | 2 |
| 4. Квантовое распределение ключа. BB84 и алгоритм Беннета. | 2 |
| 5. Практические реализации квантовых криптографических систем. Источники фотонов, линии связи, детекторы. | 2 |
| 6. Детальный разбор работающей криптографической линии. Назначение элементов и расчёт параметров. | 2 |
| 7. Уязвимости в квантовых криптографических системах. Идеальные и реальные системы. Методы борьбы со взломом квантовых криптографических систем. | 2 |
| 8. Обзор существующих систем. | 2 |
| Раздел 2 Квантовые вычисления | |
| 1. Квантовый компьютер.  Предпосылки к созданию квантового компьютера. Классы сложности алгоритмов. Предел возможностей классических компьютеров. | 2 |
| 2. Физические платформы для создания квантового компьютера.  Фотоны, сверхпроводящие элементы, нейтральные атомы и прочие системы. Современное состояние дел. | 2 |
| 3. Квантовый бит (кубит). Принцип суперпозиции, квантовая перепутанность. Описание при помощи сферы Блоха. Измерение кубита. | 2 |
| 4. Квантовая логическая операция (квантовый вентиль).  Однокубитовые вентили: тождественные преобразования, вентиль Адамара. Однокубитовые вентили, как повороты сферы Блоха. | 2 |
| 5. Многокубитовые вентили.  U, CNOT, вентиль Тоффоли, вентиль Фредкина. Понятие универсального квантового вентиля. | 2 |
| 6. Квантовые алгоритмы.  Алгоритм Дойча-Йожи, алгоритм проверки чётности, алгоритм нахождения периода. | 2 |
| 7. Квантовые алгоритмы.  Алгоритм Шора, алгоритм Гровера. | 2 |
| 8. Перепутанность в квантовых системах. Квантовая телепортация. | 2 |
| Итого: | 32 |

Лабораторные работы (32 ч)

|  |  |
| --- | --- |
| Содержание лабораторного занятия | Объем, час |
| Расчёт и сборка однофотонной линии связи. | 4 |
| Шифрование с открытым ключом | 4 |
| Попытка перехвата | 4 |
| Знакомство с платформой IBM Quantum | 4 |
| Оценка точности квантовых алгоритмов | 4 |
| Сортировка базы данных. | 4 |
| Сверхплотное кодирование | 4 |
| Детектирование перепутанных состояний | 4 |
| Итого: | 32 |

Самостоятельная работа студентов (42 ч)

|  |  |
| --- | --- |
| Перечень занятий на СРС | Объем, час |
| Изучение разделов дисциплины по учебной литературе, в том числе вопросов, не освещаемых на лекциях. Изучение предлагаемых теоретических разделов в соответствии с настоящей Программой. Учебно-методические материалы по дисциплине Шифрование и квантовая информатика выложены на странице курса в сети Интернет. | 16 |
| Подготовка к практическим занятиям, к текущему контролю знаний и промежуточной аттестации. | 18 |
| Подготовка к дифференцированному зачету. Повторение теоретического материала по вопросам, совпадающим с темами лекций | 8 |
| Итого: | 42 |

# 5. Перечень учебной литературы

***5.1 Основная литература***

1. Введение в квантовые компьютеры. Берман Г.П., Дулен Г.Д., Майньери Р., Цифринович В.И. 2019 <http://www.iprbookshop.ru/91918.html>

2. Квантовые вычисления. Эндрю Стин. 2019 <http://www.iprbookshop.ru/92042.html>

3. Введение в квантовые вычисления. Филлип Кайе, Раймон Лафламм, Мишель Моска 2019 <http://www.iprbookshop.ru/91917.html>

***5.2 Дополнительная литература***

4. Квантовая информатика и квантовые биты на основе сверхпроводниковых джозефсоновских структур: учебник. Ильичев Е. В. , Гринберг Я. С. 2013 <https://biblioclub.ru/index.php?page=book_red&id=258634>

5. Классические и квантовые вычисления. Шень А. Х. , Вялый М. Н. 2007 <https://biblioclub.ru/index.php?page=book_red&id=234673>

# 6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Для освоения дисциплины используются следующие ресурсы:

- электронная информационно-образовательная среда НГУ (ЭИОС);

- IBM Quantum;

- информационно-телекоммуникационная сеть Интернет.

Взаимодействие обучающегося с преподавателем (синхронное и (или) асинхронное) осуществляется через личный кабинет студента в ЭИОС, электронную почту, социальные сети.

***6.1 Современные профессиональные базы данных:***

*Не используются*

***6.2. Информационные справочные системы***

*Не используются*

# 7. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

***7.1 Перечень программного обеспечения***

 Для обеспечения реализации дисциплины Шифрование и квантовая информатика используется стандартный комплект программного обеспечения (ПО), включающий регулярно обновляемое лицензионное ПО Windows и MS Office и *Google Chrome,* *CPython,* *LibreOffice.*

***7.2 Информационные справочные системы***

*Не используются*

# 8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Для реализации дисциплины Шифрование и квантовая информатика используются специальные помещения:

1. Учебные аудитории для проведения занятий лекционного типа, лабораторных работ, групповых и индивидуальных консультаций, текущего контроля, промежуточной и аттестации;

2. Помещения для самостоятельной работы обучающихся;

3. Лаборатории;

4. Помещения для хранения и профилактического обслуживания учебного оборудования.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к ресурсу IBM Quantum.

Материально-техническое обеспечение образовательного процесса по дисциплине для обучающихся из числа лиц с ограниченными возможностями здоровья осуществляется согласно «Порядку организации и осуществления образовательной деятельности по образовательным программам для инвалидов и лиц с ограниченными возможностями здоровья в Новосибирском государственном университете».

# 9. Оценочные средства для проведения текущего контроля и промежуточной аттестации по дисциплине

Перечень результатов обучения по дисциплине Шифрование и квантовая информатика и индикаторов их достижения представлен в виде знаний, умений и владений в разделе 1.

***9.1 Порядок проведения текущего контроля и промежуточной аттестации по дисциплине***

***Текущий контроль успеваемости:***

Проверочные работы в начале каждой лекции по основным понятиям и определениям, изученным на предыдущих занятиях. Количество вопросов — не более 5. Время на проверочную — не более 10 минут.

Лабораторные работы после выполнения сдаются преподавателю, который оценивает достоверность полученного результата и задаёт дополнительные вопросы по сделанной работе.

***Промежуточная аттестация:***

Промежуточная аттестация по дисциплине производится: в 7 семестре в форме дифференцированного зачета. Дифференцированный зачёт проводится в виде теста, содержащего как теоретические вопросы, так и простые вычислительные задания.

***Описание критериев и шкал оценивания индикаторов достижения результатов обучения по дисциплине Шифрование и квантовая информатика***

Таблица 9.1

|  |  |  |
| --- | --- | --- |
| **Код компетенции** | **Результат обучения по дисциплине** | **Оценочное средство** |
| ОПК-2 | Знание основных направлений работы для решения задач по обработке данных и защите информации. | Проверочная работа |
| Умение производить расчёты для оценки эффективности алгоритмов и необходимых параметров устройств. | Лабораторные работы\Дифференцированный зачёт |
| Владение методами математических вычислений и построения алгоритмов. | Лабораторные работы\Дифференцированный зачёт |
| ОПК-6 | Знание основных определений и понятий в квантовой криптографии и квантовых вычислениях. | Проверочная работа |
| Умение сформулировать вопрос и критерии для отсева ненужной и недостоверной информации при проработке решения профессиональной задачи. | Проверочная работа |
| Владение навыками анализа полученного решения и методами оценки его достоверности. | Проверочная работа |
| ПК-3 | Знание устройства и принцип работы составных частей криптографических линий и вариантов физической реализации квантовых компьютеров. | Проверочная работа\Лабораторные работы\Дифференцированный зачёт |
| Умение рассчитывать требуемые характеристики криптографический линий и их составляющих. | Лабораторные работы\Дифференцированный зачёт |
| Владение методами оценки точности квантовых вычислений и определения ошибки передачи информации. | Лабораторные работы\Дифференцированный зачёт |

Таблица 9.2

|  |  |
| --- | --- |
| **Критерии оценивания результатов обучения** | **Шкала**  **оценивания** |
| **Проверочные работы**  – дан верный ответ на 5 из 5 вопросов проверочной,  – если определение или понятие сформулировано своими словами (отлично от озвученного на лекции или приведённого в литературе), то проверяется наличие ключевых слов или их синонимов и корректность их употребления,  – в вопросах, где требуется рассчитать какой-то параметр, ответ в точности соответствует необходимому значению,  **Лабораторные работы:**  – выполнены все пункты лабораторной работы,  – полученные результаты попадают в диапазон возможных значений с учётом погрешности и начальных данных,  – обучающийся может уверенно объяснить ход выполнения лабораторной работы, назвать параметры схемы и ответить на дополнительные вопросы,  **Дифференцированный зачёт:**  – уверенное владение основными понятиями и определениями и корректное их употребление в ответе,  – может достаточно полно объяснить принципы работы предоставленных схем,  – знание методов для расчёта и оценки параметров предоставленных схем и умение их применять,  – наличие исчерпывающих ответов на дополнительные вопросы. | *Отлично* |
| **Проверочные работы**  – дан верный ответ на хотя бы на 4 из 5 вопросов проверочной,  – если определение или понятие сформулировано своими словами (отлично от озвученного на лекции или приведённого в литературе), то проверяется наличие ключевых слов или их синонимов и корректность их употребления, допускаются неточности, однако общий смысл должен соответствовать правильному ответу,  – в вопросах, где требуется рассчитать какой-то параметр, ответ может не соответствовать в точности, но совпадать по порядку величины,  **Лабораторные работы:**  – выполнены все пункты лабораторной работы,  – полученные результаты могут не попадать в диапазон возможных значений с учётом погрешности и начальных данных, но должны иметь разумные величины, в соответствии с типичными значениями для таких расчётов.  – обучающийся может уверенно объяснить ход выполнения лабораторной работы, назвать параметры схемы, допускаются ошибки в ответе на дополнительные вопросы.  **Дифференцированный зачёт:**  – уверенное владение основными понятиями и определениями и корректное их употребление в ответе,  – может объяснить принципы работы предоставленных схем, допускаются ошибки, не противоречащие логике и здравому смыслу,  – знание методов для расчёта и оценки параметров предоставленных схем,  – наличие разумных ответов на дополнительные вопросы. | *Хорошо* |
| **Проверочные работы**  – дан верный ответ минимум на 3 из 5 вопросов проверочной,  – если определение или понятие сформулировано своими словами (отлично от озвученного на лекции или приведённого в литературе), общий смысл формулировки должен соответствовать правильному ответу,  – в вопросах, где требуется рассчитать какой-то параметр, ответ совпадает хотя бы по порядку величины,  **Лабораторные работы:**  – выполнено больше половины пунктов лабораторной работы,  – полученные результаты являются разумными и логически обоснованными с учётом начальных данных,  – обучающийся может самостоятельно объяснить, что и как он делал в лабораторной работе,  **Дифференцированный зачёт:**  – знает основные понятия и определения,  – может приблизительно объяснить принцип работы предоставленной схем,  – знает как найти в литературе формулы для расчёта параметров предоставленной схемы, | *Удовлетворительно* |
| **Проверочные работы**  – дан верный ответ менее чем на половину из 5 вопросов проверочной,  – не может корректно сформулировать определение или понятие даже своими словами,  – в вопросах, где требуется рассчитать какой-то параметр, ответ не соответствует верному даже по порядку величины,  **Лабораторные работы:**  – выполнено менее половины пунктов лабораторной работы,  – полученные результаты противоречат логике и здравому смыслу, сильно отличаются для типичных значений с учётом начальных условий,  – обучающийся не может самостоятельно ответить, что он делал в процессе выполнения лабораторной работы,  **Дифференцированный зачёт:**  – не владеет знанием основных понятий и определений,  – не может корректно описать принцип работы предоставленной схемы,  – не знает методы расчёта и оценки параметров предоставленной схемы и не знает, где их можно найти в литературе,  – не может ответить на дополнительные или наводящие вопросы. | *Неудовлетво-рительно* |

***Типовые контрольные задания и иные материалы, необходимые для оценки результатов обучения***

**Примеры вопросов для проверочной:**

1. Какой алгоритм используется для решения задачи факторизации?

2. Можно ли на сфере Блоха отобразить двухкубитовую операцию?

3. Что такое квантовый бит?

4. Что такое квантовая эффективность детектора?

5. Приведите формулу для расчёта периода импульсов в трейне.

6. Что такое линия задержки?

7. Что такое универсальный квантовый вентиль?

8. Напишите формулу для расчёта энергии фотона.

9. Что такое горизонтальная поляризация?

10. Что подразумевается под понятием открытый ключ?

**Примеры заданий для дифференцированного зачёта:**

1. Придумайте алгоритм сортировки произвольного массива чисел от 1 до 5.

2. Пусть квантовая система находится в базисном состоянии, соответствующем вектору |ψ>. Сколько кубитов участвует в данном состоянии?

Выписать состояние каждого кубита.

(a) |ψ> = (0, 0, 0, 1, 0, 0, 0, 0)T ;

(b) |ψ> = (0, 0, 0, 0, 0, 0, 1, 0)T ;

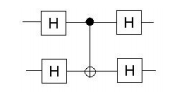
(c) |ψ> = √ 1 2 (0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)T

3. Разработайте квантовую схему, состоящую из однокубитовых вентилей и вентиля CNOT, воздействующий на второй кубит, которая осуществляет преобразование:

|00> → 1 /√ 2 (|01> − |10>);

|11> → 1 /√ 2 (|00> + |11>).

4. Дана квантовая схема:

Найти результат воздействия этой схемы на состояние 01.

5. Покажите, что если вентиль CNOT применяется к Адамаровскому базису (то есть с использованием преобразования Адамара до и после применения вентиля CNOT), то контролируемый и контролирующий кубиты меняются местами.

6. Предположим, что Алиса и Боб осуществляют плотное кодирование. Злоумышленник Ева перехватывает передаваемый Алисой кубит и затем пересылает его Бобу. Может ли Ева сохранить факт своего вмешательства в тайне от Боба? Может ли она узнать закодированное Алисой сообщение? Если да – почему? Если нет – почему?

7. Опишите принцип работы протокола SARG04.

Оценочные материалы по промежуточной аттестации (приложение 2), предназначенные для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС, хранятся на кафедре-разработчике РПД в печатном и электронном виде.

**Лист актуализации рабочей программы дисциплины**

**«Шифрование и квантовая информатика»**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Характеристика внесенных изменений (с указанием пунктов документа) | Дата и №  протокола Ученого совета ВКИ | Подпись  ответственного |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |