

Рабочая программа дисциплины

1. Название дисциплины: Физические методы взлома систем квантовой связи

2. Уровень высшего образования – магистратура

3. Направление подготовки: 03.04.02 Физика (магистратура)

4. Аннотация:

Курс «Физические методы взлома систем квантовой связи» является профильной дисциплиной магистерской программы «Квантовая криптография и квантовая связь». Дисциплина призвана дать представление слушателям об известных методах атаки на оборудование в системах квантового распределения ключей. Учет такого рода атак и их понимание является ключевым элементом при разработке практических систем квантовой криптографии, а также и при разработке новых перспективных протоколов квантовой коммуникации.

5. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся (указывается согласно рабочему плану):

Объем дисциплины составляет 2 зачетные единицы, всего 72 часа, из которых 36 часов составляет контактная работа обучающегося с преподавателем (18 часов занятия лекционного типа, 16 часов занятия семинарского типа, 2 часа коллоквиумов), 36 часов составляет самостоятельная работа обучающегося.

6. Формируемые компетенции и входные требования для освоения дисциплины, предварительные условия:

НАЗВАНИЕ КОМПЕТЕНЦИЙ:

СПК-1 Способность свободно владеть профессиональными знаниями для анализа и синтеза физической информации в области физики квантовых вычислений.

СПК-2 Способность к поиску, критическому анализу, обобщению и систематизации научной информации в области физики квантовых вычислений.

СПК-3 Способность организовывать и планировать исследования, ставить конкретные задачи научных исследований в области физики квантовых вычислений, и решать их с помощью современной аппаратуры и оборудования.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Для того чтобы формирование данных компетенций было возможно, обучающийся, приступивший к освоению образовательной программы, должен:

- **ЗНАТЬ:** основные методы научно-исследовательской деятельности.
- **УМЕТЬ:** выделять и систематизировать основные идеи в научных текстах; критически оценивать любую поступающую информацию, вне зависимости от источника; избегать автоматического применения стандартных формул и приемов при решении задач.
- **ВЛАДЕТЬ:** навыками сбора, обработки, анализа и систематизации информации по теме исследования; навыками выбора методов и средств решения задач исследования.

Для освоения дисциплины необходимы знания и умения, приобретаемые в рамках дисциплин «Квантовая механика», «Основы квантовой оптики», а также математических дисциплин «Линейная алгебра» и «Теория вероятности и стохастические процессы». Желательно также предварительно освоить дисциплину «Криптография и элементы теории информации».

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

Наименование и краткое содержание разделов и тем дисциплины, форма промежуточной аттестации по дисциплине	Всего, часы	В том числе						
		Контактная работа (работа во взаимодействии с преподавателем), часы из них				Самостоятельная работа обучающегося, часы из них		
		Занятия лекционного типа	Занятия семинарского типа	Учебные занятия, направленные на проведение текущего контроля успеваемости коллоквиумы, практические контрольные занятия и др.*	Всего	Выполнение домашних заданий	Подготовка рефератов и т.п.	Всего
1. Атаки на протоколы квантовой криптографии. §1. Краткий обзор известных атак на протоколы квантового распределения ключей. Индивидуальные атаки, когерентные атаки, атака со светоделителем, атака с разделением по числу фотонов, атака путем измерений с определенным исходом. Граница Холево для бинарного квантового канала. §2. Принципиальные различия между однофотонными протоколами и протоколами на когерентных состояниях. Применимость вышеуказанных атак в этих двух случаях.		5	3		8	2 часа Знакомство с обзорами по системам квантовой криптографии 2 часа изучение конструктивной атаки на однофотонный протокол BB84, достигающий теоретической границы по числу ошибок.		4

§3. Протоколы с состояниями-ловушками (decoy state).								
2. Атаки с активным зондированием §4. Реализация атак с активным зондированием. Сравнение однопроходных и двухпроходных схем квантовой криптографии. §5. Методы защиты от атак с активным зондированием. Изоляторы, быстрые ключи, разрыв канала. Измерение энергии импульсов в двухпроходных схемах. §6. Протоколы без активных элементов на приемной стороне. Генерация квантовых состояний с помощью injection locking.		5	3		8	2 часа Знакомство с оригинальными статьями по взлому систем квантовой криптографии 4 часа Повторение лекционного материала по теме «Атаки на протоколы квантовой криптографии».		6
3. Специфические атаки на оборудование §7. Атака с подменой фазы (phase remapping). §8. Атака с временным сдвигом §9. Атака с ослеплением однофотонных детекторов. Варианты защиты от данной атаки. Мониторинг напряжения на однофотонном детекторе. Различия между поляризационным и фазовым кодированием. §10. Атака с рассогласованием детекторов (detector mismatch) §11. Атака с лазерным повреждением детекторов		4	4	2 часа Коллоквиум по пройденным темам	10	6 часов Подготовка к коллоквиуму		6
4. Атаки типа man in the middle §11. Суть атаки и способы защиты от нее. Имитозащита.		4	2		6	1 час Самостоятельное		5

Аутентификация абонентов.						изучение методов аутентификации с использованием шифров с открытым ключом. 4 часа Повторение лекционного материала по теме «Специфические атаки на оборудование».		
Промежуточная аттестация - зачет			4		4	15 часов Подготовка к промежуточной аттестации (зачету).		15
Итого		18	16	2	36			36

* Текущий контроль успеваемости в рамках занятий семинарского типа реализуется в форме обсуждения.

8. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине:

8.1 Основная и дополнительная литература доступная студентам через Интернет или по запросу лектору.

9. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Типовые контрольные вопросы и темы для обсуждения:

1. Индивидуальные и когерентные атаки на системы квантовой криптографии
2. Различия между однофотонными протоколами и протоколами на когерентных состояниях.
3. Активное зондирование фазовых модуляторов
4. Защита от атак с зондированием в двухпроходных схемах
5. Атака с подменой фазы
6. Атаки с ослеплением однофотонных детекторов
7. Атаки на рассогласовании детекторов

8. Атака с лазерным повреждением детекторов
9. Атака с временным сдвигом
10. Проблема аутентификации в квантовой криптографии
11. Генерация квантовых состояний с помощью injection locking
12. Протоколы без активных элементов на приемной стороне.

Типовые вопросы к зачету:

1. Возможные атаки на однофотонные протоколы. Примеры на базе протокола BB84
2. Атака с разделением по числу фотонов. Применимость. Пример на одном из протоколов.
3. Атака со светоделителем. Граница Холево. Применимость данного вида атак.
4. Атака на измерениях с определенным исходом. Пример на конкретном протоколе.
5. Вероятность успеха измерений с определенным исходом для случая с состояниями из протоколов B92 и BB84
6. Атака с активным зондированием в однопроходных схемах
7. Атака с активным зондированием в двухпроходных схемах
8. Методы защиты от атак с активным зондированием
9. Генерация квантовых состояний с помощью injection locking
10. Протоколы без активных элементов на приемной стороне.
11. Атака с подменой фазы
12. Атаки с ослеплением однофотонных детекторов
13. Атаки на рассогласовании детекторов
14. Атака с лазерным повреждением детекторов
15. Атака с временным сдвигом
16. Различие между поляризационным и фазовым кодированием для атаки с ослеплением детекторов
17. Атаки типа man in the middle
18. Проблема аутентификации абонентов в системах квантовой криптографии
19. Протоколы с состояниями-ловушками (decoy state QKD). Примеры и отличие от традиционных протоколов.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ПОКАЗАТЕЛИ ДОСТИЖЕНИЯ ЗАДАННОГО УРОВНЯ ОСВОЕНИЯ КОМПЕТЕНЦИЙ)

ВЛАДЕТЬ: профессиональными знаниями для анализа и синтеза физической информации в области физики квантовых вычислений (В1, СПК-1).

ВЛАДЕТЬ: навыками поиска, критического анализа, обобщения и систематизации научной информации в области физики квантовых вычислений (В2, СПК-2).

ВЛАДЕТЬ: навыками анализа методологических проблем, возникающих при планировании, организации и решении конкретных исследовательских задач в области физики квантовых вычислений (В3, СПК-3).

УМЕТЬ: анализировать альтернативные варианты решения исследовательских задач в области физики квантовых вычислений и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов (У1, СПК-1).

УМЕТЬ: осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области физики квантовых вычислений (У2, СПК-2).

УМЕТЬ: организовывать и планировать исследования, ставить конкретные задачи научных исследований в области физики квантовых вычислений, и решать их с помощью современной аппаратуры и оборудования (У3, СПК-3).

ЗНАТЬ: методы анализа и оценки современных научных достижений, а также методы генерирования новой физической информации при решении исследовательских и практических задач в области физики квантовых вычислений (З1, СПК-1).

ЗНАТЬ: способы критического анализа и систематизации научной информации при решении исследовательских задач в области физики квантовых вычислений (З2, СПК-2).

ЗНАТЬ: методы организации и планирования исследований в области физики квантовых вычислений, включая способы решения задач с помощью современной аппаратуры и оборудования (З3, СПК-3).

Планируемые результаты	Критерии оценивания результатов обучения
------------------------	--

обучения (показатели достижения заданного уровня освоения компетенций)	1	2	3	4	5
<i>ВЛАДЕТЬ:</i> профессиональными знаниями для анализа и синтеза физической информации в области физики квантовых вычислений (B1, СПК-1).	Отсутствие навыков	Фрагментарное применение навыков анализа и синтеза физической информации в области физики квантовых вычислений	В целом успешное, но не систематическое применение навыков анализа и синтеза физической инфор- мации в области физики квантовых вычислений	В целом успешное, но содержащее отдельные пробелы применение навыков анализа и синтеза физической информации в области физики квантовых вычислений	Успешное и систематическое применение навыков анализа и синтеза физической информации в области физики квантовых вычислений
<i>ВЛАДЕТЬ:</i> навыками поиска, критического анализа, обобщения и систематизации научной информации в области физики квантовых вычислений (B2, СПК-2).	Отсутствие навыков	Фрагментарное применение навыков поиска, критического анализа, обобщения и систематизации научной информации в области физики квантовых вычислений	В целом успешное, но не систематическое применение навыков поиска, критического анализа, обобщения и систематизации научной информации в области физики квантовых вычислений	В целом успешное, но содержащее отдельные пробелы применение навыков поиска, критического анализа, обобщения и сис- тематизации научной информации в области физики квантовых вычислений	Успешное и систематическое применение навыков поиска, критического анализа, обобщения и систематизации научной информации в области физики квантовых вычислений
<i>ВЛАДЕТЬ:</i> навыками анализа методологических проблем, возникающих	Отсутствие навыков	Фрагментарное применение навыков анализа методологи- ческих проблем, возникающих при	В целом успешное, но не систематическое применение навыков анализа методологи- ческих проблем,	В целом успешное, но содержащее отдельные пробелы применение навыков анализа методологических проблем, возникающих при	Успешное и систематическое применение навыков анали- за методологических проблем, возникающих

при планировании, организации и решении конкретных исследовательских задач в области физики квантовых вычислений (ВЗ, СПК-3).		планировании, организации и решении конкретных исследовательских задач в области физики квантовых вычислений	возникающих при планировании, организации и решении конкретных исследовательских задач в области физики квантовых вычислений	планировании, организации и решении конкретных исследовательских задач в области физики квантовых вычислений	при планировании, организации и решении конкретных исследовательских задач в области физики квантовых вычислений
<i>УМЕТЬ:</i> анализировать альтернативные варианты решения исследовательских задач в области физики квантовых вычислений и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов (У1, СПК-1).	Отсутствие умения	Фрагментарное проявление умения анализировать альтернативные варианты решения исследовательских задач в области физики квантовых вычислений и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов	В целом успешное, но не систематическое проявление умения анализировать альтернативные варианты решения исследовательских задач в области физики квантовых вычислений и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов	В целом успешное, но содержащее отдельные пробелы проявление умения анализировать альтернативные варианты решения исследовательских задач в области физики квантовых вычислений и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов	Успешное и систематическое проявление умения анализировать альтернативные варианты решения исследовательских задач в области физики квантовых вычислений и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов

<i>УМЕТЬ:</i> осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области физики квантовых вычислений (У2, СПК-2).	Отсутствие умения	Фрагментарное проявление умения осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области физики квантовых вычислений	В целом успешное, но не систематическое проявление умения осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области физики квантовых вычислений	В целом успешное, но содержащее отдельные пробелы проявление умения осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области физики квантовых вычислений	Успешное и систематическое проявление умения осуществлять поиск, критический анализ, обобщать и систематизировать научную информацию в области физики квантовых вычислений
<i>УМЕТЬ:</i> организовывать и планировать исследования, ставить конкретные задачи научных исследований в области физики квантовых вычислений, и решать их с помощью современной аппаратуры и оборудования (У3, СПК-3)	Отсутствие умения	Фрагментарное проявление умения организовывать и планировать исследования, ставить конкретные задачи научных исследований в области физики квантовых вычислений, и решать их с помощью современной аппаратуры и оборудования	В целом успешное, но не систематическое проявление умения организовывать и планировать исследования, ставить конкретные задачи научных исследований в области физики квантовых вычислений, и решать их с помощью современной аппаратуры и оборудования	В целом успешное, но содержащее отдельные пробелы проявление умения организовывать и планировать исследования, ставить конкретные задачи научных исследований в области физики квантовых вычислений, и решать их с помощью современной аппаратуры и оборудования	Успешное и систематическое проявление умения организовывать и планировать исследования, ставить конкретные задачи научных исследований в области физики квантовых вычислений, и решать их с помощью современной аппаратуры и оборудования

<i>ЗНАТЬ:</i> методы анализа и оценки современных научных достижений, а также методы генерирования новой физической информации при решении исследовательских и практических задач в области физики квантовых вычислений (31, СПК-1)	Отсутствие знаний	Фрагментарное проявление знаний методов анализа и оценки современных научных достижений, а также методов генерирования новой физической информации при решении исследовательских и практических задач в области физики квантовых вычислений	В целом успешное, но не систематическое проявление знаний методов анализа и оценки современных научных достижений, а также методов генерирования новой физической информации при решении исследовательских и практических задач в области физики квантовых вычислений	В целом успешное, но содержащее отдельные пробелы проявление знаний методов анализа и оценки современных научных достижений, а также методов генерирования новой физической информации при решении исследовательских и практических задач в области физики квантовых вычислений	Успешное и систематическое проявление знаний методов анализа и оценки современных научных достижений, а также методов генерирования новой физической информации при решении исследовательских и практических задач в области физики квантовых вычислений
<i>ЗНАТЬ:</i> способы критического анализа и систематизации научной информации при решении исследовательских задач в области физики квантовых вычислений (32, СПК-2).	Отсутствие знаний	Фрагментарное проявление знаний способов критического анализа и систематизации научной информации при решении исследовательских задач в области физики квантовых вычислений	В целом успешное, но не систематическое проявление знаний способов критического анализа и систематизации научной информации при решении исследовательских задач в области физики квантовых вычислений	В целом успешное, но содержащее отдельные пробелы проявление знаний способов критического анализа и систематизации научной информации при решении исследовательских задач в области физики квантовых вычислений	Успешное и систематическое проявление знаний способов критического анализа и систематизации научной информации при решении исследовательских задач в области физики квантовых вычислений

ЗНАТЬ: методы организации и планирования исследований в области физики квантовых вычислений, включая способы решения задач с помощью современной аппаратуры и оборудования (33, СПК-3)	Отсутствие знаний	Фрагментарное проявление знаний методов организации и планирования исследований в области физики квантовых вычислений, включая способы решения задач с помощью современной аппаратуры и оборудования	В целом успешное, но не систематическое проявление знаний методов организации и планирования исследований в области физики квантовых вычислений, включая способы решения задач с помощью современной аппаратуры и оборудования	В целом успешное, но содержащее отдельные пробелы проявление знаний методов организации и планирования исследований в области физики квантовых вычислений, включая способы решения задач с помощью современной аппаратуры и оборудования	Успешное и систематическое проявление знаний методов организации и планирования исследований в области физики квантовых вычислений, включая способы решения задач с помощью современной аппаратуры и оборудования
--	-------------------	--	--	--	---

10. Перечень основной и дополнительной учебной литературы

Основная литература

1. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys., vol. 81, no. 3, pp. 1301-1350, 2009.
2. N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs "Attacks on practical quantum key distribution systems (and how to prevent them)" Contemp. Phys., Vol. 57, No. 3, pp. 366–387, 2016.
3. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys., vol. 74, no. 1, pp. 145-195, 2002.

Дополнительная литература

4. F. Xu, B. Qi, and H.-K. Lo, "Experimental demonstration of phase remapping attack in a practical quantum key distribution system," New J. Phys., vol. 12, no. 11, p. 113026, 2010.
5. C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, "Phase-remapping attack in practical quantum-key-distribution systems," Phys. Rev. A, vol. 75, no. 3, p. 032314, 2007.

6. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 78, no. 4, p. 042333, 2008.
7. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photon.*, vol. 4, no. 10, pp. 686-689, 2010.
8. N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Trojan-horse attacks threaten the security of practical quantum cryptography," *New J. Phys.* 16 (2014), p. 123030.
9. I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system", *Nat. Commun.* 2 (2011), p. 349.
10. V. Makarov and D. Hjelle, "Faked states attack on quantum cryptosystems", *J. Modern Opt.* 52 (2005), pp. 691–705.
11. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Thermal blinding of gated detectors in quantum cryptography", *Opt. Express* 18 (2010), pp. 27938–27954.
12. C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "After-gate attack on a quantum cryptosystem", *New J. Phys.* 13 (2011), p. 013043.
13. L. Lydersen, M.K. Akhlaghi, H.A. Majedi, J. Skaar, and V. Makarov, "Controlling a superconducting nanowire singlephoton detector using tailored bright illumination", *New J. Phys.* 13 (2011), p. 113042.
14. V. Makarov, "Controlling passively quenched single photon detectors by bright light", *New J. Phys.* 11 (2009), p. 065003.
15. S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, "Controlling an actively-quenched single photon detector with bright light", *Opt. Express* 19 (2011), pp. 23590–23600.
16. A.N. Bugge, S. Sauge, A.M.M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, "Laser damage helps the eavesdropper in quantum cryptography", *Phys. Rev. Lett.* 112 (2014), p. 70503.
17. V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems", *Phys. Rev. A* 74 (2006), p. 022313.
18. H.W. Li, S. Wang, J.Z. Huang, W. Chen, Z.Q. Yin, F.Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.C. Guo, W.S. Bao, and Z.F. Han, "Attacking a practical quantumkey- distribution system with wavelength-dependent beamsplitter and multiwavelength sources", *Phys. Rev. A* 84 (2011), p. 062308.
19. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-keydistribution systems", *Phys. Rev. A* 73 (2006), p. 022320.
20. A. Vakhitov, V. Makarov, and D. Hjelle, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography", *J. Modern Opt.* 48 (2001), pp. 2023–2038.

21. J.Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z.Q. Yin, S. Wang, W. Chen, G.C. Guo, and Z.F. Han, "Quantum hacking on quantum key distribution using homodyne detection", Phys. Rev. A 89 (2014), p. 032304.

11. Перечень ресурсов Интернет необходимых для освоения дисциплины:

- <https://arxiv.org/>

12. Методические указания для обучающихся по освоению дисциплины

Для освоения дисциплины необходимо посещение интерактивных занятий (лекций и семинаров) и регулярная самостоятельная работа в течение семестра.

13. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости):

- средства дистанционного сопровождения учебного процесса в форме сайта с избранными материалами лекций и семинарских занятий.
- лекции читаются с использованием современных мультимедийных возможностей и проекционного оборудования.

14. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

В соответствии с требованиями п. 5.3. образовательного стандарта МГУ по направлению подготовки «Физика». Любая аудитория, оснащенная проекционным оборудованием с возможностью подключения к ноутбуку, экраном, и учебной доской.