Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Новосибирский национальный исследовательский
государственный университет» (Новосибирский государственный университет, НГУ)

Факультет информационных технологий

СОГЛАСОВАНО
Декан ФИТ НГУ
_____ М.М. Лаврентьев
«18» апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Вычисления в криптографии

Направление подготовки: 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Направленность (профиль): Квантовые технологии и криптография

Форма обучения: очная
Год обучения: 2, семестр: 3

№	Вид деятельности	Семестр
		3
1	Лекции, час.	32
2	Практические занятия, час.	32
3	Лабораторные занятия, час.	
4	Занятий в контактной форме без учета промежуточной аттестации, час, из них	64
5	в электронной форме, час.	
6	из них аудиторных занятий, час.	64
7	из них в активной и интерактивной форме, час.	64
8	консультаций, час.	
9	Самостоятельная работа, час.	42
10	в том числе на выполнение письменных работ, час	20
11	Форма аттестации (экзамен, зачет, дифференцированный зачет), час	ДЗ 2
12	Всего зачетных единиц[1]	3

Новосибирск 2022

[1] С учетом выделенных часов на промежуточную аттестацию

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта (ФГОС) высшего образования - магистратура по направлению подготовки 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА.

Федеральный государственный образовательный стандарт (ФГОС) высшего образования по направлению подготовки магистратуры 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА введен в действие приказом Минобрнауки 19.09.2017 № 918.

Место дисциплины в структуре учебного плана: Блок 1 Дисциплины (модули), часть, формируемая участниками образовательных отношений, Блока 1 дисциплин (модулей) и дисциплина по выбору.

Рабочая программа дисциплины утверждена решением Ученого совета факультета информационных технологий от 28.03.2022 протокол № 84.

Программу разработали:

доцент кафедры компьютерных систем ФИТ
кандидат физико-математических наук — Н.Н. Токарева

Старший преподаватель кафедры параллельных вычислений ФИТ,
кандидат физико-математических наук — К.В.Калгин

Заведующий кафедрой систем информатики ФИТ,
доктор физико-математических наук — М.М. Лаврентьев

Ответственный за образовательную программу:
доцент КвЭл ФФ НГУ ФФ НГУ
кандидат физико-математических наук — И.И.Бетеров

Аннотация к рабочей программе дисциплины
«Вычисления в криптографии»

Дисциплина «Вычисления в криптографии» реализуется в рамках образовательной программы высшего образования – программы магистратуры 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): КВАНТОВЫЕ ТЕХНОЛОГИИ И КРИПТОГРАФИЯ по очной форме обучения на английском языке.

Место в образовательной программе: Дисциплина «Вычисления в криптографии» развивает знания, умения и навыки, сформированные у обучающихся по результатам изучения следующих дисциплин: «Дискретная математика», «Теория вероятности и математическая статистика», «Теория информации и криптография».

Дисциплина «Вычисления в криптографии» реализуется в 3 семестре в рамках части, формируемой участниками образовательных отношений, Блока 1 дисциплин (модулей) и является дисциплиной по выбору.

Дисциплина «Вычисления в криптографии» направлена на формирование компетенций:

Способен выполнять фундаментальные и прикладные работы поискового, теоретического и экспериментального характера (ПКС-1), в части следующих индикаторов достижения компетенции:

ПКС-1.1. Применяет актуальные модели и подходы в области профессиональной деятельности

ПКС-1.2. Комбинирует и адаптирует существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности

ПКС-1.3 Применяет на практике программные средства и платформы информационных технологий для разработки и реализации математических моделей, проведение их анализа при решении задач в области профессиональной деятельности

Перечень основных разделов дисциплины:

1. Способы представление булевой и векторной функции. Преобразования. Криптографические свойства. Перебор функций.
2. Средства автоматизации описания и решения задач (SAT-решатели, SMT-решатели, Transalg, Cryptominisat, Bosphorus).

При освоении дисциплины студенты выполняют следующие виды учебной работы: лекции, практические занятия, самостоятельная работа. Самостоятельная работа включает подготовку к практическим занятиям.

Общий объем дисциплины – 3 зачетных единиц (108 часов).

Правила аттестации по дисциплине. Текущий контроль по дисциплине «Вычисления в криптографии» осуществляется при сдаче практических работ. Выполненные практические работы входят в портфолио студента.

Промежуточная аттестация по дисциплине проводится в конце 3 семестра в форме дифференцированного зачета. Оценка выставляется по результатам оценивания портфолио, в которое входят практические работы, выполненные и защищённые на протяжении семестра. При сдаче 80% практических работ выставляется оценка “отлично”, при сдаче 65% практических работ выставляется оценка “хорошо”, при сдаче 50% -

“удовлетворительно”. При сдаче менее 50% практических работ выставляется оценка «неудовлетворительно».

Результаты промежуточной аттестации по дисциплине оцениваются по шкале «неудовлетворительно», «удовлетворительно», «хорошо», «отлично». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации. Оценка «отлично» соответствует продвинутому уровню сформированности компетенции. Оценка «хорошо» соответствует базовому уровню сформированности компетенции. Оценка «удовлетворительно» соответствует пороговому уровню сформированности компетенции.

Учебно-методическое обеспечение дисциплины.

Учебно-методическое обеспечение дисциплины представлено в рабочей программе дисциплины в виде методических рекомендаций по подготовке и выполнению практических работ.

Учебно-методические материалы по дисциплине выкладываются на электронный ресурс, создаваемый для каждого нового набора

1. Внешние требования к дисциплине

Таблица 1.1

Компетенция ПКС-1 Способен выполнять фундаментальные и прикладные работы поискового, теоретического и экспериментального характера, *в части следующих индикаторов достижения компетенции*:	
ПКС-1.1	Применяет актуальные модели и подходы в области профессиональной деятельности
ПКС-1.2	Комбинирует и адаптирует существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности
ПКС-1.3	Применяет на практике программные средства и платформы информационных технологий для разработки и реализации математических моделей, проведение их анализа при решении задач в области профессиональной деятельности

2. Требования к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**		
	Лекции	**Практические работы**	**Самостоятельная работа**
ПКС-1.1. Применяет актуальные модели и подходы в области профессиональной деятельности			
1. Знать способы представления булевых и векторных функций, подходы к формулированию и решению криптографических задач	+	+	+
2. Знать современные программные средства решения криптографических задач	+	+	+
ПКС-1.2. Комбинирует и адаптирует существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности			
3. Уметь обосновать выбора описания булевых и векторных функций для решения определенной задачи.	+	+	+
4. Знать существующие средства автоматизации описания и решения криптографических задач.	+	+	+
5. Уметь обосновать выбор программного средства решения криптографической задачи.	+	+	+
ПКС-1.3 Применяет на практике программные средства и платформы информационных технологий для разработки и реализации математических моделей, проведение их анализа при решении задач в области профессиональной деятельности			
6. Уметь реализовывать алгоритмы решения криптографических задач	+	+	+
7. Иметь навыки описания криптографических задач различными способами		+	+

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения
Семестр: 3			
1. Введение. Вычислительные задачи в криптографии.	0	2	1 2
2. Представление булевой и векторной функции. Преобразования между разными способами представления	0	4	1 2 3
3. Тесты проверки последовательности на случайность	0	2	2 4
4. Криптографические свойства узлов замены (S-блоков) в симметричных шифрах	0	4	2 4
5. Перечисление функций. Полный перебор, перебор в глубину с отсечениями.	0	4	1 2 3
6. SAT-решатели. Введение, базовые алгоритмы, существующие решения.	0	8	2 5 6
7. Реализация атаки угадай-и-вычисли.	0	4	2 3 4
8. Средства автоматизации описания и решения задач криптографии.	0	4	2 4 5 6
Итого		**32**	

Таблица 3.2

Темы практических работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 3				
Тема 1. Преобразование между разными способами представления (описания) функций.	2	6	1 2 3	Обучающиеся изучают вспомогательный математический аппарат, используемый для описания функций (АНФ, КНФ, бинарные диаграммы, таблица истинности). Реализуют программы преобразования.
Тема 2. Вычисление криптографических свойств S-блоков	2	6	3 4	Реализуют программы вычисления криптографических свойств (алгебраическая иммунность, нелинейность, дифференциальная равномерность). Оценивают свойства S-блока известных шифров.
Тема 3. Проведение атаки угадай-и-вычисли с помощью SAT-решателя	6	10	5 6 7	Используют Transalg, Cryptominisat и др. средства для описания шифров, SAT-решатели для проведения этапа «вычисли».
Тема 4. Автоматический	6	10	5 6 7	Определение устойчивости

анализ S-блоков с помощью SMT-решателей.				S-блоков к линейному и дифференциальному криптоанализу.
Итого	**16**	**32**		

4. Самостоятельная работа студентов

Таблица 4.1

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 3				
1	Изучение разделов дисциплины по учебной литературе, в том числе вопросов, не освещаемых на лекциях	1-7	17	
	Изучение предлагаемых теоретических разделов в соответствии с настоящей Программой. Учебно-методические материалы по дисциплине выложены на странице курса в сети Интернет			
2	Подготовка к практическим занятиям, к текущему контролю знаний	1-7	20	
	Выполнение заданий			
3	Подготовка к дифференцированному зачету	1-7	5	
	Повторение теоретического материала по вопросам, совпадающим с темами лекций			
	Итого		42	

5. Образовательные технологии

В ходе реализации учебного процесса по дисциплине проводятся лекционные и практические занятия. Темы, рассматриваемые на лекциях и изучаемые самостоятельно, закрепляются на практических занятиях.

В ходе реализации учебного процесса по дисциплине применяются следующие интерактивные формы организации учебных занятий (таблица 5.1).

Таблица 5.1

1	Портфолио	ПКС-1
Формируемые умения: 1. Знать способы представления булевых и векторных функций. 2. Знать подходы к формулированию и решению криптографических задач. 3. Уметь использовать разные способы описания булевых и векторных функций и обосновывать их выбор. 4. Уметь вычислять криптографические свойства S-блоков. 5. Знать существующие средства автоматизации описания и решения криптографических задач и обосновывать их выбор. 6. Уметь использовать существующие средства решения криптографических задач. 7. Иметь навыки описания криптографических задач различными способами и обосновывать их выбор.		
Краткое описание применения: студенты ведут портфолио (коллекцию работ), которое является основой для проведения аттестации по дисциплине.		

Для организации и контроля самостоятельной работы студентов применяются информационно-коммуникационные технологии (таблица 5.2).

Таблица 5.2

Информирование	kalginkv@gmail.com
Консультирование	kalginkv@gmail.com
Контроль	kalginkv@gmail.com
Размещение учебных материалов	crypto.nsu.ru

6. Правила аттестации студентов по учебной дисциплине

По дисциплине «Вычисления в криптографии» проводится текущая и промежуточная аттестация (итоговая по дисциплине).

Текущий контроль осуществляется во время практических занятий по количеству выполненных и защищенных работ. Выполненные работы входят в портфолио студента.

Промежуточная аттестация (итоговая по дисциплине) проводится по завершению семестра в форме дифференцированного зачёта. Оценка за освоение дисциплины выставляется по результатам оценивания портфолио работ студента, которое включает выполненные и защищённые практические работы.

Результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

При сдаче 80% практических работ выставляется оценка “отлично”, при сдаче 65% практических работ выставляется оценка “хорошо”, при сдаче 50% - “удовлетворительно”. При сдаче менее 50% практических работ выставляется оценка «неудовлетворительно».

В таблице 6.1 представлено соответствие форм аттестации заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.1

Коды компетенций ФГОС	**Результаты обучения**	**Формы аттестации**	
		1 этап - портфолио	**2 этап – дифференцированный зачет**
ПКС-1	ПКС-1.1. Применяет актуальные модели и подходы в области профессиональной деятельности	+	+
	ПКС-1.2. Комбинирует и адаптирует существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	+	+
	ПКС-1.3 Применяет на практике программные средства и платформы информационных технологий для разработки и реализации математических моделей,	+	+

	проведение их анализа при решении задач в области профессиональной деятельности		

Требования к структуре и содержанию портфолио, оценочные средства, а также критерии оценки сформированности компетенций и освоения дисциплины в целом, представлены в Фонде оценочных средств, являющемся приложением 1 к настоящей рабочей программе дисциплины.

7. Перечень учебной литературы

1. Токарева Н.Н. Симметричная криптография: краткий курс. Учебное пособие. М-во образования и науки РФ, Новосиб гос. ун-т, Мех.-мат. фак., Каф. теорет. кибернетики. Новосибирск, 2012. 234 с. http://e-lib.nsu.ru/dsweb/Get/Resource-1222/page001.pdf

8. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины

При освоении дисциплины используются следующие ресурсы:

- электронная информационно-образовательная среда НГУ (ЭИОС);
- образовательные интернет-порталы;
- информационно-телекоммуникационная сеть Интернет.

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

Таблица 8.1

№ п/п	Наименование Интернет-ресурса	Краткое описание
1	https://ebooks.iospress.nl/volume/handbook-of-satisfiability-second-edition	Книга C. P. Gomes and A. Sabharwal. Handbook of Satisfiability. 2009.
2	https://github.com/Z3Prover/z3	Документация SMT-решателя Z3
3	https://github.com/msoos/cryptominisat	Документация cryptominisat5

9. Учебно-методическое и программное обеспечение дисциплины

9.1. Перечень учебно-методических материалов по самостоятельной работе обучающихся

Для обеспечения самостоятельной работы обучающихся при изучении дисциплины используются методические рекомендаций по подготовке и выполнению работ

Методические рекомендаций по подготовке и выполнению практических работ.

Процесс подготовки практической работы выглядит следующим образом.

1. Каждое занятие в терминальном классе посвящено одной из практических работ. На нем излагается необходимая для выполнения работы теория, и обговариваются сложности, которые могут возникнуть в ходе выполнения работы. На занятии можно проконсультироваться с преподавателем по поводу неясных студенту деталей работы.
2. Описание практической работы и необходимые для её выполнения материалы (описание алгоритмов, использующийся математический аппарат, криптографические термины и теория) доступны по ссылке в методических материалах.

3. Практическая работа может быть реализована на любом языке программирования, но наиболее подходящие языки могут разниться в зависимости от работы. Например, удобно использовать Python для практических, в которых используется длинная арифметика или символьные вычисления, но не требуется производительность.

4. По практической работе необходимо написать отчет и отправить его преподавателю. В отчете должна содержаться информация о практической работе и об особенностях ее реализации, ссылка на код (если практическая работа сдается очно на занятии, то ссылка не обязательна), инструкция, позволяющая провести тестирование работы, временная сложность (в зависимости от конкретной работы, это может быть теоретическая оценка сложности алгоритма или время выполнения на какой-либо машине при входных данных некоторой длины).

5. При защите практической студент должен рассказать о проделанной работе и ответить на вопросы, касающиеся смысла работы, минимальной необходимой теории, а также на вопросы по коду. Преподаватель также может попросить внести небольшие изменения в код.

9.2. Программное обеспечение

Для обеспечения реализации дисциплины используется стандартный комплект программного обеспечения (ПО), включающий регулярно обновляемое лицензионное ПО Windows и MS Office.

Перечень специализированного программного обеспечения для изучения дисциплины представлен в таблице 9.1.

Специализированное программное обеспечение Таблица 9.1

№	Наименование ПО	Назначение
1	Microsoft Visual Studio Professional 2019	Среда разработки приложений
2	Putty	Доступ к удаленному компьютеру с установленной ОС Linux

10. Профессиональные базы данных и информационные справочные системы

1. Полнотекстовые журналы Springer Journals, электронные книги, коллекция научных биомедицинских и биологических протоколов SpringerProtocols, коллекция научных материалов в области физических наук и инжиниринга SpringerMaterials, реферативная БД по чистой и прикладной математике zbMATH.
2. Электронные ресурсы Web of Science Core Collection (Thomson Reuters Scientific LLC.), Journal Citation Reports + ESI
3. Лицензионные материалы на сайте eLibrary.ru
4. Материалы международных конференций по теории информации и криптографии: ISIT, EUROCRYPT, CRYPTO, FSE, ASIACRYPT, SIBECRYPT, BFA и др.

11. Материально-техническое обеспечение

Для реализации дисциплины используются специальные помещения:

1. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля, промежуточной и итоговой аттестации;

2. Помещения для самостоятельной работы обучающихся;

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 в электронную информационно-образовательную среду НГУ.

Таблица 11.1

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Для проведения лекционных занятий
2	Компьютерный класс (с выходом в Internet)	Для проведения практических занятий и организации самостоятельной работы

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».

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Новосибирский национальный исследовательский
государственный университет» (Новосибирский государственный университет, НГУ)

Факультет информационных технологий

СОГЛАСОВАНО
Декан ФИТ НГУ
М.М. Лаврентьев
«18» апреля 2022 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
по дисциплине Вычисления в криптографии

Направление подготовки: 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА.

Направленность (профиль): Квантовые технологии и криптография
Квалификация: Магистр

Форма обучения: очная

Год обучения: 2, семестр 3

Форма аттестации	Семестр
Дифзачет	3

Новосибирск 2022

Фонд оценочных средств промежуточной аттестации является **Приложением 1** к рабочей программе дисциплины «Вычисления в криптографии», реализуемой в рамках образовательной программы высшего образования – программы магистратуры 09.04.01 Информатика и вычислительная техника, направленность (профиль): Квантовые технологии и криптография

Фонд оценочных средств промежуточной аттестации по дисциплине утвержден решением Ученого совета факультета информационных технологий протокол № 84 от 28.03.2022

Разработчик:
доцент кафедры компьютерных систем ФИТ
кандидат физико-математических наук Н.Н. Токарева

Старший преподаватель кафедры параллельных вычислений ФИТ,
кандидат физико-математических наук К.В.Калгин

Заведующий кафедрой систем информатики ФИТ,
доктор физико-математических наук М.М. Лаврентьев

Ответственный за образовательную программу:
Доцент кафедры квантовой электроники ФФ,
кандидат физико-математических наук И.И.Бетеров

1. Содержание и порядок проведения промежуточной аттестации по дисциплине

1.1. Общая характеристика содержания промежуточной аттестации

Промежуточная аттестация по дисциплине «Вычисления в криптографии» проводится по завершению периода освоения образовательной программы (семестра) для оценки сформированности компетенций в части следующих индикаторов достижения компетенции (таблица П1.1).

Таблица П1.1

Коды компетенций ФГОС	Компетенции, формируемые в рамках дисциплины «Вычисления в криптографии»	Семестр 3	
		портфолио	дифзачет
ПКС-1 Способен выполнять фундаментальные и прикладные работы поискового, теоретического и экспериментального характера			
ПКС-1.1	Применяет актуальные модели и подходы в области профессиональной деятельности	+	+
ПКС-1.2	Комбинирует и адаптирует существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	+	+
ПКС-1.3	Применяет на практике программные средства и платформы информационных технологий для разработки и реализации математических моделей, проведение их анализа при решении задач в области профессиональной деятельности	+	+

Тематика вопросов к диф.зачету соответствует избранным разделам (темам) дисциплины «Вычисления в криптографии»

Способы представление булевой и векторной функции.

Преобразования.

Криптографические свойства.

Перебор функций.

Средства автоматизации описания и решения задач (SAT-решатели, SMT-решатели, Transalg, Bosphorus).

Промежуточная аттестация включает 2 этапа:

1. Портфолио.
2. Дифзачет.

Все компетенции, формируемые в рамках дисциплины, оцениваются как через портфолио, так и на дифзачете.

1.2. Порядок проведения промежуточной аттестации по дисциплине

Промежуточная аттестация проводится в форме дифзачета и включает 2 этапа: портфолио и дифзачет. Необходимым условием для прохождения промежуточной аттестации является

оценка «зачтено» по результатам выполненного портфолио. Для оценивания портфолио студенту необходимо сдать все работы, входящие в структуру портфолио.

Портфолио включает выполнение заданий по темам практических занятий.

Дифзачет проводится в устной форме, в аудитории, студентам разрешено пользоваться бумагой для записей и авторучкой. Во время проведения дифзачета студенту разрешается использовать справочники, учебную и научную литературу, компьютеры. В процессе ответа на вопросы дифзачета студенту могут быть заданы дополнительные вопросы по темам дисциплины.

2. Требования к структуре и содержанию фонда оценочных средств промежуточной аттестации по дисциплине

Перечень оценочных средств, применяемых на каждом этапе проведения промежуточной аттестации по дисциплине, представлен в таблице П1.2.

Таблица П1.2

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Этап 1 - портфолио			
1.	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или нескольких учебных дисциплинах	Структура портфолио
Этап 2 – Дифзачет			
2	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины

2.1. Требования к структуре и содержанию оценочных средств аттестации в семестре

Текущая аттестация по дисциплине «Вычисления в криптографии» проводится в форме портфолио. Промежуточная аттестация проводится в формате дифзачета.

2.1.1 Требования к структуре и содержанию портфолио
Портфолио включает защиту заданий на практических занятиях.

Оценка за курс выставляется по результатам дифзачета. Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

2.1.2 Перечень вопросов дифзачета 3 семестра

Преобразование между разными способами представления (описания) функций.

Вычисление криптографических свойств S-блоков

Проведение атаки угадай-и-вычисли с помощью SAT-решателя

Автоматический анализ S-блоков с помощью SMT-решателей.

Набор вопросов к дифзачету формируется и утверждается в установленном порядке в начале учебного года при наличии контингента обучающихся, завершающих освоение дисциплины «Вычисления в криптографии» в текущем учебном году.

3. **Критерии оценки сформированности компетенций в рамках промежуточной аттестации по дисциплине**

Таблица П1.5

Шифр компетенций	**Структурные элементы оценочных средств**	**Показатель сформированности**	**Не сформирован**	**Пороговый уровень**	**Базовый уровень**	**Продвинутый уровень**
ПКС-1	Портфолио (этап 1), Дифзачет (этап 2)	ПКС-1.1. Применяет актуальные модели и подходы в области профессиональной деятельности	Не знает актуальные модели и подходы в области профессиональной деятельности	Допускает грубые ошибки, слабо знает способы представления булевых и векторных функций, подходы к формулированию и решению криптографических задач	Знает на базовом уровне способы представления булевых и векторных функций, подходы к формулированию и решению криптографических задач	Уверенно знает способы представления булевых и векторных функций, подходы к формулированию и решению криптографических задач, современные программные средства решения криптографических задач
ПКС-1	Портфолио (этап 1), Дифзачет (этап 2)	ПКС-1.2. Комбинирует и адаптирует существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	Не умеет комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения	Демонстрирует слабые умения обосновать выбор описания булевых и векторных функций для решения определенной задачи.	Умеет обосновать выбор описания булевых и векторных функций для решения определенной задачи, выбор программного средства решения криптографической задачи, допускает несущественные погрешности	Умеет обосновать выбор описания булевых и векторных функций для решения определенной задачи, выбор программного средства решения криптографической задачи.

			задач в области профессиональной деятельности с учетом требований информационной безопасности			
ПКС-1	Портфолио (этап 1), Дифзачет (этап 2)	ПКС-1.3 Применяет на практике программные средства и платформы информационных технологий для разработки и реализации математических моделей, проведение их анализа при решении задач в области профессиональной деятельности	Не умеет применять на практике программные средства и платформы информационных технологий для разработки и реализации математических моделей, проведение их анализа при решении	Слабо владеет навыками реализовывать алгоритмы решения криптографических задач	Владеет навыками реализовывать алгоритмы решения криптографических задач, описания криптографических задач различными способами	Уверенно владеет навыками реализовывать алгоритмы решения криптографических задач, описания криптографических задач различными способами

			задач в области профессиональной деятельности			

4. **Критерии выставления оценок по результатам промежуточной аттестации по дисциплине**

В соответствии с учебным планом устанавливаются следующие формы контроля:

Результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Оценка «отлично» соответствует продвинутому уровню сформированности компетенции.

Оценка «хорошо» соответствует базовому уровню сформированности компетенции.

Оценка «удовлетворительно» соответствует пороговому уровню сформированности компетенции.

Оценка «неудовлетворительно» выставляется, если хотя бы одна компетенция не сформирована.

Итоговая оценка результатов промежуточной аттестации выставляется как оценка за дифзачет.