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

«26» апреля 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Современные вычислительные системы для решения задач криптографии и информационной безопасности

Направление подготовки: 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Направленность (профиль): Программная инженерия и компьютерные науки

Форма обучения: очная
Год обучения: 3, семестр: 5

№	Вид деятельности	Семестр
		5
1	Лекции, час.	16
2	Практические занятия, час.	
3	Лабораторные занятия, час.	32
4	Занятий в контактной форме без учета промежуточной аттестации, час, из них	48
5	в электронной форме, час.	
6	из них аудиторных занятий, час.	48
7	из них в активной и интерактивной форме, час.	16
8	консультаций, час.	
9	Самостоятельная работа, час.	60
10	в том числе на выполнение письменных работ, час	
11	Форма аттестации (экзамен, зачет, дифференцированный зачет), час	ДЗ
12	Всего зачетных единиц[1]	3

Новосибирск 2021

[1] С учетом выделенных часов на промежуточную аттестацию

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта (ФГОС) высшего образования - бакалавриат по направлению подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА.

Федеральный государственный образовательный стандарт (ФГОС) высшего образования - бакалавриат по направлению подготовки 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА введен в действие приказом Минобрнауки от 19.09.2017 № 929.

Место дисциплины в структуре учебного плана: Блок ФТД Факультативы, факультативная дисциплина.

Рабочая программа дисциплины утверждена решением Ученого совета факультета информационных технологий от 26.04.2021, протокол № 80.

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 компьютерных систем ФИТ,
кандидат технических наук Б.Н. Пищик

Ответственный за образовательную программу:

Доцент кафедры систем информатики ФИТ,
кандидат технических наук А.А. Романенко

Аннотация к рабочей программе дисциплины

«Современные вычислительные системы для решения задач криптографии и информационной безопасности»

Дисциплина «Современные вычислительные системы для решения задач криптографии и информационной безопасности» реализуется в рамках образовательной программы высшего образования – программы бакалавриата 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): ПРОГРАММНАЯ ИНЖЕНЕРИЯ И КОМПЬЮТЕРНЫЕ НАУКИ;

Место в образовательной программе: Дисциплина «Современные вычислительные системы для решения задач криптографии и информационной безопасности» развивает знания, умения и навыки, сформированные у обучающихся по результатам изучения следующих дисциплин: «Информатика», «Программирование», «Дискретная математика».

Дисциплина «Современные вычислительные системы для решения задач криптографии и информационной безопасности» реализуется в 5 семестре в рамках Блока ФТД Факультативы и является факультативной дисциплиной.

Дисциплина «Современные вычислительные системы для решения задач криптографии и информационной безопасности» направлена на формирование компетенций:

Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности (ОПК-2), в части следующих индикаторов достижения компетенции:

ОПК-2.1 Знать: современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.

ОПК-2.2 Уметь: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.

ОПК-2.3 Владеть: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач 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).
3. Средства автоматизированного анализа шифров, их элементов и программного кода на основе Z3, angr.

При освоении дисциплины студенты выполняют следующие виды учебной работы: лекции, лабораторные работы, самостоятельная работа. Самостоятельная работа включает подготовку к лабораторным работам.

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

Правила аттестации по дисциплине. Текущий контроль по дисциплине «Современные вычислительные системы для решения задач криптографии» осуществляется при сдаче лабораторных работ. Выполненные лабораторные работы входят в портфолио студента.

Промежуточная аттестация по дисциплине проводится в конце 5 семестра в форме дифференцированного зачета. Оценка выставляется по результатам оценивания портфолио, в которое входят лабораторные работы, выполненные и защищённые на протяжении семестра. При сдаче 80% лабораторных работ выставляется оценка “отлично”, при сдаче 65% лабораторных работ выставляется оценка “хорошо”, при сдаче 50% - “удовлетворительно”. При сдаче менее 50% лабораторных 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 лабораторных работ.

Методические рекомендации по дисциплине «Современные вычислительные системы для решения задач криптографии и информационной безопасности» в электронной информационно-образовательной среде НГУ:
https://drive.google.com/drive/folders/1llCzNfWnETtRpqa_HdfAJ3U1vewWdPta?usp=sharing

1. **Внешние требования к дисциплине**

Таблица 1.1

Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности (ОПК-2), в части следующих индикаторов достижения компетенции:
ОПК-2.1 Знать: современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.
ОПК-2.2 Уметь: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.
ОПК-2.3 Владеть: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач 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	**Лабораторные работы**	**Самостоятельная работа**
ОПК-2.1 Знать: современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.			
1. Знать способы представления булевых и векторных функций	+	+	+
2. Знать подходы к формулированию и решению криптографических задач	+	+	+
ОПК-2.2 Уметь: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.			
3. Уметь использовать разные способы описания булевых и векторных функций	+	+	+
4. Уметь вычислять криптографические свойства S-блоков	+	+	+
ОПК-2.3 Владеть: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.			
5. Знать существующие средства автоматизации описания и решения криптографических задач	+	+	+
6. Уметь использовать существующие средства 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: 5			
1. Введение. Вычислительные задачи в криптографии.	0	1	1 2
2. Представление булевой и векторной функции. Преобразования между разными способами представления	0	2	1 2 3
3. Тесты проверки последовательности на случайность	0	1	2 4
4. Криптографические свойства узлов замены (S-блоков) в симметричных шифрах	0	2	2 4
5. Перечисление функций. Полный перебор, перебор в глубину с отсечениями.	0	2	1 2 3
6. SAT-решатели. Введение, базовые алгоритмы, существующие решения.	0	2	2 5 6
7. Реализация атаки угадай-и-вычисли.	0	2	2 3 4
8. Средства автоматизации описания и решения задач криптографии.	0	2	2 4 5 6
9. Введение в обратную разработку программ. Применение SMT-решателей при обратной разработке программ.	0	2	2 4 5 6
Итого		**16**	

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 5				
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	4	7	5 6 7	Используют Transalg, Cryptominisat и др. средства для описания шифров, SAT-

				решатели для проведения этапа «вычисли».
Тема 4. Автоматический анализ S-блоков с помощью SMT-решателей.	4	7	5 6 7	Определение устойчивости S-блоков к линейному и дифференциальному криптоанализу.
Тема 5. Выявление корректного ввода программы путем ручного анализа кода и применения SMT-решателя	4	6	5 6 7	Использование SMT-решателей Z3, angr при анализе программного кода, в котором реализован неизвестный шифр.
Итого	**16**	**32**		

4. Самостоятельная работа студентов

Таблица 4.1

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 5				
1	Подготовка к лабораторным занятиям.	1,2,3,4,5,6,7	60	0
	Дополнительный самостоятельный разбор материалов, необходимых для выполнения лабораторных работ. https://drive.google.com/drive/folders/1llCzNfWnETtRpqa_HdfAJ3U1vewWdPta?usp=sharing			
	Итого		**60**	

5. Образовательные технологии

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

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

Таблица 5.1

1	Портфолио	ОПК-2
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. 4. Уметь вычислять криптографические свойства S-блоков. 5. Знать существующие средства автоматизации описания и решения криптографических задач. 6. Уметь использовать существующие средства решения криптографических задач. 7. Иметь навыки описания криптографических задач различными способами.		
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 https://drive.google.com/drive/folders/1llCzNfWnETtRpqa_HdfAJ3U1vewWdPta?usp=sharing

6. Правила аттестации студентов по учебной дисциплине

По дисциплине «Современные вычислительные системы для решения задач криптографии и информационной безопасности» проводится текущая и промежуточная аттестация (итоговая по дисциплине).

Текущий контроль осуществляется во время лабораторных занятий по количеству выполненных и защищенных лабораторных работ. Выполненные лабораторные 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 лабораторные работы.

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

При сдаче 80% лабораторных работ выставляется оценка “отлично”, при сдаче 65% лабораторных работ выставляется оценка “хорошо”, при сдаче 50% - “удовлетворительно”. При сдаче менее 50% лабораторных 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**
		дифференцированный зачет
		портфолио
ОПК-2	ОПК-2.1 Знать: современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.	+
	ОПК-2.2 Уметь: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.	+
	ОПК-2.3 Владеть: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач 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
4	https://www.coursera.org/learn/cryptography-boolean-functions	Курс «Cryptography: Boolean functions and related problems» на платформе Coursera от НГУ

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 лабораторных работ https://drive.google.com/drive/folders/1llCzNfWnETtRpqa_HdfAJ3U1vewWdPta?usp=sharing

Описание криптографических свойств булевых и векторных функций можно найти в пособии 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

Методические рекомендаций по подготовке и выполнению лабораторных работ.

Процесс подготовки лабораторной работы выглядит следующим образом.

1. Каждое занятие в терминальном классе посвящено одной из лабораторных 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 лабораторной работы и необходимые для её выполнения материалы (описание алгоритмов, использующийся математический аппарат, криптографические термины и теория) доступны по ссылке в методических материалах.
3. Лабораторная работа может быть реализована на любом языке программирования, но наиболее подходящие языки могут разниться в зависимости от работы. Например, удобно использовать Python для лабораторных, в которых используется длинная арифметика, но не требуется производительность.
4. По лабораторной работе необходимо написать отчет и отправить его преподавателю. В отчете должна содержаться информация о лабораторной работе и об особенностях ее реализации, ссылка на код (если лабораторная 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 лабораторной 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. БД Scopus (Elsevier)
4. Лицензионные материалы на сайте eLibrary.ru
5. 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 лабораторных 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».

Лист актуализации рабочей программы дисциплины

«Современные вычислительные системы для решения задач криптографии и информационной безопасности»

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

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
«26» апреля 2021 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

«Современные вычислительные системы для решения задач криптографии и информационной безопасности»

Направление подготовки: 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Направленность (профиль): Программная инженерия и компьютерные науки

Квалификация: бакалавр

Форма обучения: очная Год обучения: 3, семестр 5

Форма аттестации	Семестр
Дифференцированный зачет	5

Новосибирск 2021

Фонд оценочных средств промежуточной аттестации по дисциплине является **Приложением 1** к рабочей программе дисциплины «**Современные вычислительные системы для решения задач криптографии и информационной безопасности**», реализуемой в рамках образовательной программы высшего образования – программы бакалавриата 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): Программная инженерия и компьютерные науки.

Фонд оценочных средств промежуточной аттестации по дисциплине утвержден решением ученого совета факультета информационных технологий, протокол № 80 от 26.04.2021.

Разработчики:
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 компьютерных систем ФИТ,
кандидат технических наук Б.Н. Пищик

Ответственный за образовательную программу:

доцент кафедры систем информатики ФИТ,

кандидат технических наук А.А. Романенко

1. Содержание и порядок проведения промежуточной аттестации по дисциплине

1.1. Общая характеристика содержания промежуточной аттестации

Промежуточная аттестация по дисциплине «**Современные вычислительные системы для решения задач криптографии и информационной безопасности**» проводится по завершению 5-го семестра (дифференциальный зачет) для оценки сформированности компетенций в части следующих индикаторов достижения компетенции (таблица П1.1).

Таблица П1.1

Код	Компетенции, формируемые в рамках дисциплины «Современные вычислительные системы для решения задач криптографии и информационной безопасности»	Семестр 5 Дифференцированный зачет Портфолио
	ОПК-2. Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	
ОПК-2.1	Знать: современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	+
ОПК-2.2	Уметь: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	+
ОПК-2.3	Владеть: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	+

Промежуточная аттестация осуществляется в форме дифференцированного зачета. Оценка выставляется по результатам оценивания портфолио.

1.2. Порядок проведения промежуточной аттестации по дисциплине

Промежуточная аттестация по дисциплине проводится в конце 5 семестра в форме дифференцированного зачета. Оценка выставляется по результатам оценивания портфолио, в которое входят лабораторные работы, выполненные и защищённые на протяжении семестра. При сдаче 80% лабораторных работ выставляется оценка “отлично”, при сдаче 65% лабораторных работ выставляется оценка “хорошо”, при сдаче 50% - “удовлетворительно”. При сдаче менее 50% лабораторных 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.

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
Семестр 5			
Дифференцированный зачет			
1	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или нескольких учебных дисциплинах.	Структура портфолио

2.1 Требования к структуре и содержанию оценочных средств аттестации

Требования к структуре и содержанию портфолио

Портфолио должно содержать результаты выполненных и защищенных лабораторных работ по следующим темам:

1. Преобразование между разными способами представления (описания) функций.
2. Вычисление криптографических свойств S-блоков.
3. Проведение атаки угадай-и-вычисли с помощью SAT-решателя.
4. Автоматический анализ S-блоков с помощью SMT-решателей.
5. Выявление корректного ввода программы путем ручного анализа кода и применения SMT-решателя.

Пример описания лабораторной работы.

Выберете два представления функции из списка: АНФ, КНФ, таблица истинности, представление над полем, ROBDD. Реализуйте программу, переводящую из одного представления функции в другое и обратно. Предложите формат файла для каждого из способов представления функции. Реализуйте чтение и запись в файл в соответствующем формате.

Отчет о проделанной работе должен содержать: программу, описание алгоритма перевода между способами представления функции, описание формата текстового файла, описание используемых структур данных, время работы алгоритма и объём используемой памяти, изменение размера файла на различных функциях и S-блоках.

Лабораторная работа считается сданной после успешной защиты отчета о проделанной работе, демонстрации работы программы и обсуждении деталей реализации и работы программы.

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

Таблица П1.3

Шифр компе-тенций	**Структурные элементы оценочных средств**	**Показатель сформированности**	**Не сформирован (2 балла)**	**Пороговый уровень (3 балла)**	**Базовый уровень (4 балла)**	**Продвинутый (5 баллов)**
ОПК-2	Портфолио	ОПК-2.1 Знать: современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	Имеет фрагментарные знания о криптографических задачах и булевых функциях	Знает подходы к формулированию и решению криптографических задач и способы представления булевых функций, но затрудняется при их использовании	Знает подходы к формулированию и решению криптографических задач и способы представления булевых функций и умеет с небольшими пробелами их использовать	Знает подходы к формулированию и решению криптографических задач и способы представления булевых функций и умеет их использовать
ОПК-2	Портфолио	ОПК-2.2 Уметь: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	Имеет фрагментарные знания о способах описания булевых функций и о криптографических свойствах S-блоков	Умеет использовать разные способы описания булевых функций и S-блоков, но студент испытывает затруднения, допускает ошибки, нуждается в подсказках	Умеет использовать разные способы описания булевых функций и S-блоков, но испытывает некоторые затруднения	Умеет использовать разные способы описания булевых функций и S-блоков
ОПК-2	Портфолио	ОПК-2.3 Владеть: навыками применения современных информационных технологий и программных средств, в	Имеет фрагментарные знания о решении и описании криптографичес	Знает существующие средства автоматизации описания и решения	Знает существующие средства автоматизации описания и решения криптографических задач и умеет с	Знает существующие средства автоматизации описания и решения криптографических задач и умеет их

		том числе отечественного производства, при решении задач профессиональной деятельности	ких задач	криптографических задач, но затрудняется при их использовании	небольшими пробелами их использовать	использовать

4. Критерии выставления оценок по результатам промежуточной аттестации по дисциплине

В 5 семестре результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Оценка выставляется по результатам оценивания портфолио, в которое входят лабораторные работы, выполненные и защищённые на протяжении семестра. При сдаче 80% лабораторных работ выставляется оценка “отлично”, при сдаче 65% лабораторных работ выставляется оценка “хорошо”, при сдаче 50% - “удовлетворительно”. При сдаче менее 50% лабораторных работ выставляется оценка «неудовлетворительно».

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 компетенция не сформирована.

Лист актуализации фонда оценочных средств промежуточной аттестации по дисциплине «Современные вычислительные системы для решения задач криптографии и информационной безопасности»

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