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
«03» июля 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптография для информационных технологий

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

Форма обучения: очная
Год обучения: 4, семестр: 7

№	Вид деятельности	Семестр
		7
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	66
5	в электронной форме, час.	
6	из них аудиторных занятий, час.	64
7	из них в активной и интерактивной форме, час.	32
8	консультаций, час.	2
9	Самостоятельная работа, час.	76
10	в том числе на выполнение письменных работ, час	
11	Форма аттестации (экзамен, зачет, дифференцированный зачет), час	Э 2
12	Всего зачетных единиц[1]	4

Новосибирск 2019

[1] С учетом выделенных часов на промежуточную аттестацию

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): ПРОГРАММНАЯ ИНЖЕНЕРИЯ И КОМПЬЮТЕРНЫЕ НАУКИ, по очной форме обучения на русском языке.

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

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

Рабочая программа дисциплины утверждена решением Ученого совета факультета информационных технологий от 02.07.2019, протокол № 75.

Программу разработал:

Профессор кафедры компьютерных систем ФИТ,
Доктор технических наук — Б.Я.Рябко

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
«Криптография для информационных технологий»

Дисциплина «Криптография для информационных технологий» реализуется в рамках образовательной программы высшего образования – программы бакалавриата 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): ПРОГРАММНАЯ ИНЖЕНЕРИЯ И КОМПЬЮТЕРНЫЕ НАУКИ по очной форме обучения на русском языке.

Место в образовательной программе: Дисциплина «Криптография для информационных технологий» развивает знания, умения и навыки, сформированные у обучающихся по результатам изучения следующих дисциплин:
«Информатика», «Дискретная математика», «Теория вероятностей и математическая статистика», «Математическая логика и теория алгоритмов», «Программирование», «Введение в теорию кодирования».
Дисциплина «Криптография для информационных технологий» является базовой для: «Учебная практика», «Производственная практика».

Дисциплина «Криптография для информационных технологий» реализуется в 7 семестре в рамках части, формируемой участниками образовательных отношений, дисциплин (модулей) Блока 1 и является дисциплиной по выбору.

Дисциплина «Криптография для информационных технологий» направлена на формирование компетенций:
Способен разрабатывать компоненты системных программных продуктов (ПКС-2), в части следующих индикаторов достижений компетенции:
ПКС-2.3 Уметь применять знания в области разработки ПО в предметной области

Перечень основных разделов дисциплины: цели применения криптографических методов в информационных технологиях, криптография с открытым ключом и основные протоколы, симметричная криптография и теория Шеннона, технология «блокчейн» и криптовалюты, блоковые и потоковые шифры, хэшфункции.

При освоении дисциплины студенты выполняют следующие виды учебной работы: лекции, практические занятия, консультации, самостоятельная работа. В учебном процессе предусматривается использование активных и интерактивных форм проведения занятий. В том числе, предполагаются исследовательские темы, связанные с разработкой эффективных алгоритмов.

Самостоятельная работа включает: подготовку к практическим занятиям по разделам дисциплины, подготовку презентаций докладов, написание рефератов, подготовку к экзамену.

Общий объем дисциплины – 4 зачетных единиц (144 часа).

Правила аттестации по дисциплине. Текущий контроль по дисциплине «Криптография для информационных технологий» осуществляется на практических занятиях и заключается в презентации и защите докладов по основным разделам дисциплины, по результатам которых выставляется оценка «зачтено» или «не зачтено». Оценка «зачтено» по результатам защиты докладов является одним из условий успешного прохождения промежуточной аттестации.

Промежуточная аттестация по дисциплине «Криптография для информационных технологий» проводится по завершению каждого периода ее освоения. Промежуточная аттестация по дисциплине проводится в форме представления и защиты отчета по

результатам ее прохождения. По результатам аттестации выставляется оценка «зачтено» или «не зачтено».

В 7 семестре оценка за освоение дисциплины выставляется по результатам оценивания портфолио работ студента, которое включает:

1) выполненные лабораторные работы;

2) решение задач по темам.

Оценка за дисциплину в 7 семестре выставляется в формате «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.

В 7 семестре аттестация по дисциплине включает 2 этапа:

1) портфолио;

2) экзамен.

Учебно-методическое обеспечение дисциплины.

Учебно-методический комплекс по дисциплине «Криптография для информационных технологий» представлен следующей литературой:

Рябко, Борис Яковлевич. Криптография в информационном мире / Б.Я. Рябко, А.Н. Фионов. Москва : Горячая линия - Телеком, 2018. 300 с. : ил. ; 22 см. ISBN 978-5-9912-0729-4. (18 экз.)

1. **Внешние требования к дисциплине**

Таблица 1.1

Компетенция ПКС -2 Способен разрабатывать компоненты системных программных продуктов, *в части следующих индикаторов достижения компетенции:*
ПКС-2.3 Уметь применять знания в области разработки ПО в предметной области

2. Требования к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**		
	Лекции	**Практики / семинары**	**Самостоятельная работа**
ПКС-2.3 Уметь применять знания в области разработки ПО в предметной области			
1. Знать современные программно-аппаратные комплексы систем защиты информации.	+	+	+
2. Уметь использовать современные программные средства и обеспечивать их высокую эффективность в системах защиты информации.		+	+

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	**Активные формы, час. (входит в общее кол-во часов)**	**Часы**	**Ссылки на результаты обучения**
Семестр: 7			
1. Симметричные системы шифрования		10	1
2. Криптосистемы с открытым ключом		10	1
3. Блокчейн и криптовалюты		12	1
Итого:		**32**	

Таблица 3.2

Темы практических занятий	Активные формы, час. (входит в общее кол-во часов)	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 7				
Тема 1. Симметричные системы шифрования	10	10	1,2	Обучающиеся изучают блоковые и потоковые шифры.
Тема 2. Криптосистемы с открытым ключом	10	10	2	Обучающиеся изучают основные криптосистемы с открытым ключом
Тема 3. Блокчейн и криптовалюты	12	12	2	Обучающиеся изучают блокчейн и криптовалюты
Итого:	**32**	**32**		

4. Самостоятельная работа студентов

Таблица 4.1

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 7				
1	Подготовка к практическим занятиям по теме 1.	1,2	10	
	Решение задач по книге: Рябко, Борис Яковлевич. Криптография в информационном мире / Б.Я. Рябко, А.Н. Фионов. Москва : Горячая линия - Телеком, 2018. 300 с. : ил. ; 22 см. ISBN 978-5-9912-0729-4			
2	Подготовка к практическим занятиям по теме 2.	1,2,	10	
	Решение задач по книге: Рябко, Борис Яковлевич. Криптография в информационном мире / Б.Я. Рябко, А.Н. Фионов. Москва : Горячая линия - Телеком, 2018. 300 с. : ил. ; 22 см. ISBN 978-5-9912-0729-4			
3	Подготовка к практическим занятиям по теме 3.	1,2	12	
	Решение задач по книге Рябко, Борис Яковлевич. Криптография в информационном мире / Б.Я. Рябко, А.Н. Фионов. Москва : Горячая линия - Телеком, 2018. 300 с. : ил. ; 22 см. ISBN 978-5-9912-0729-4			
4	Подготовка реферата.	1	10	
	Оформление результатов обсуждения на практических занятиях в форме реферата.			
5	Подготовка презентации доклада.	1,2	10	
6	Подготовка к экзамену	1,2	24	2
	Подготовка к экзамену по вопросам, представленным в фонде оценочных средств, являющихся приложением к рабочей программе дисциплины.			
	Итого:		**76**	**2**

5. Образовательные технологии

В ходе реализации учебного процесса по дисциплине проводятся лекционные и семинарские занятия. Темы, рассматриваемые на лекциях и изучаемые самостоятельно, закрепляются на семинарах, по вопросам, вызывающим затруднения, проводятся консультации.

Лекции проводятся в виде обзоров, высвечивающих темы для самостоятельного изучения по учебно-методической литературе. Практические занятия проводятся в интерактивной форме. На практических занятиях решаются задачи, иллюстрирующие работу изучаемых методов, а также демонстрируются и обсуждаются разработанные программы. Самостоятельная работа включает в себя изучение материала по литературе и написание компьютерных программ, реализующих основные изучаемые алгоритмы. Интерактивные практические занятия могут проводиться в двух режимах. Большинство изучаемых криптографических алгоритмов предполагает наличие двух участников взаимодействия. Эти два участника могут создаваться путем деления учебной группы на две части, либо образовываться в параллельно работающих парах студентов. Вначале рекомендуется использовать деление группы на две части, т.к. это упрощает контроль преподавателем правильности действий. По мере укрепления навыков можно переходить к работе в парах. Все действия участников должны протоколироваться на бумаге, чтобы затем была возможность провести общее обсуждение и анализ.

Все разрабатываемые студентами компьютерные программы, реализующие изучаемые методы, имеют исследовательскую составляющую, заключающуюся в выборе тех или иных алгоритмов реализации вычислений и в измерении некоторых практических параметров получающихся криптосистем.

Таблица 5.1

1	Технологии проблемного обучения	**ПКС-2.3**
Формируемые умения: Уметь оценивать преимущества и недостатки применяемых обучающимся методов в сравнении с методами, уже используемыми в системах защиты информации.		
Краткое описание применения: Постановка под руководством преподавателя проблемных задач и активная самостоятельная деятельность обучающихся по их разрешению, сопровождающаяся обсуждением результатов.		
2	Портфолио	**ПКС-2.3**
Формируемые умения: Уметь использовать изученные криптографические методы в системах защиты информации.		
Краткое описание применения: студенты ведут портфолио (коллекцию выполненных лабораторных работ), которое является основой для проведения аттестации по дисциплине.		

Для организации и контроля самостоятельной работы студентов, а также проведения консультаций применяются информационно-коммуникационные технологии (таблица 5.2).

Таблица 5.2

Информирование	Адрес почты,b.riabko@g.nsu.ru
Консультирование	Адрес почты b.riabko@g.nsu.ru
Контроль	Адрес почты b.riabko@g.nsu.ru
Размещение учебных материалов	-

6. Правила аттестации студентов по учебной дисциплине

По дисциплине «Криптография для информационных технологий» проводится текущая и промежуточная аттестация (итоговая по дисциплине).

Текущая аттестация по дисциплине «Криптография для информационных технологий» осуществляется на практических занятиях и заключается в презентации и защите докладов по каждой теме практических занятий. В ходе обучения каждый студент должен подготовить презентации докладов по каждому разделу самостоятельной работы и публично выступить с ними, защищая полученные результаты в ходе обсуждения и дискуссии. По результатам текущей аттестации выставляется оценка «зачтено» или «не зачтено». Оценка «зачтено» по результатам защиты докладов является одним из условий успешного прохождения промежуточной аттестации.

Для получения оценки «зачтено» презентация и доклад на каждую тему, соответствующую разделам дисциплины в каждом семестре, должна быть выполнена и защищена в полном соответствии с предъявляемыми требованиями.

Промежуточная аттестация (итоговая по дисциплине) проводится по завершению каждого периода ее освоения (семестра) в виде защиты индивидуального проекта в формате портфолио, в состав которого включаются все работы, выполненные студентом в ходе изучения дисциплины. Завершает портфолио итоговая рефлексивная работа, направленная на переосмысление и оценку содержания дисциплины «Криптография для информационных технологий» и реализованной в его рамках учебной деятельности.

По результатам освоения дисциплины «Криптография для информационных технологий» результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

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

Таблица 6.1

Коды компетенций ФГОС	**Результаты обучения**	**Формы аттестации**	
		Портфолио	**Экзамен**
ПКС-2.3	**ПКС-2.3** Уметь применять знания в области разработки ПО в предметной области	+	+

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. Литература

1. Ryabko, Boris. Compression-Based Methods of Statistical Analysis and Prediction of Time Series / Boris Ryabko, Jaakko Astola, Mikhail Malyutov. [Printforce] : Springer, [2016]. 144 p. : Ill. ; 24 cm. ISBN 978-3-319-32251-3 ((alk. paper)) . ISBN 978-3-319-32253-7 ((eBook)) (10 экз)

Интернет-ресурсы

Таблица 7.1

№ п/п	Наименование Интернет-ресурса	Краткое описание
1	Журнал «Вестник НГУ. Серия: Информационные технологии»	Полнотекстовые электронные копии статей в области вычислительный

	[Электронный ресурс]. – Режим доступа: https://journals.nsu.ru/jit/ . – Загл. с экрана	методов (с 2006 года).
2	Сайт International Association for Cryptologic Research [Электронный ресурс]. – Режим доступа: https://iacr.org/	Сайт содержит статьи по криптографии.

8. Учебно-методическое и программное обеспечение дисциплины

8.1. Учебно-методическое обеспечение

Рябко, Борис Яковлевич. Криптография в информационном мире / Б.Я. Рябко, А.Н. Фионов. Москва : Горячая линия - Телеком, 2018. 300 с. : ил. ; 22 см. ISBN 978-5-9912-0729-4. (18 экз.)

8.2. Программное обеспечение

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

Специализированное ПО не требуется.

9. Профессиональные базы данных и информационные справочные системы

1. Полнотекстовые журналы Springer Journals за 1997-2019 г., электронные книги (2005-2018 гг.),
2. Электронные ресурсы Web of Science Core Collection (Thomson Reuters Scientific LLC.), Journal Citation Reports + ESI
3. Лицензионные материалы на сайте eLibrary.ru
4. Правовая БД «Консультант Плюс»
5. Правовая БД «Гарант»

10. Материально-техническое обеспечение

Таблица 10.1

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

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
«Криптография для информационных технологий»

№	Характеристика внесенных изменений (с указанием пунктов документа)	Дата и № протокола Ученого совета ФИТ	Подпись ответственного
1.	Актуализирована на 2020-2021 уч.год	22.07.2020 №77	

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
«03» июля 2019 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
по дисциплине Криптография для информационных технологий

Направление подготовки: 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Направленность (профиль): Программная инженерия и компьютерные науки

Квалификация: бакалавр

Форма обучения: очная

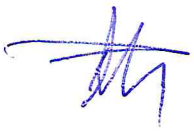
Год обучения: 4, семестр 7

Форма аттестации	Семестр
Экзамен	7

Новосибирск 2019

Фонд оценочных средств промежуточной аттестации по дисциплине является **Приложением 1** к рабочей программе дисциплины «Криптография для информационных технологий», 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 № 75 от 02.07.2019.

Разработчики:
Проф. кафедры компьютерных систем ФИТ,
Доктор технических наук  Б.Я.Рябко

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

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 «Криптография для информационных технологий» проводится по завершению периода освоения образовательной программы (семестра) для оценки сформированности компетенций в части следующих индикаторов достижения компетенции (таблица П1.1).

Таблица П1.1

Код	Компетенции, формируемые в рамках дисциплины «Введение в организацию распределенных вычислений»	Семестр 7	
		Портфолио	Экзамен
ПКС-2 Способен разрабатывать компоненты системных программных продуктов			
ПКС-2.3	Уметь применять знания в области разработки ПО в предметной области	+	+

Промежуточная аттестация включает 2 этапа:

1. Портфолио.
2. Устный экзамен.

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

Тематика контрольных работ, образующих портфолио, и экзаменационных вопросов включает следующие темы (разделы): криптография с открытым ключом, блоковые и потоковые шифры, генераторы случайных чисел и тесты для них, блокчейн и криптовалюты .

1.2. Порядок проведения промежуточной аттестации по дисциплине

Промежуточная аттестация проводится в форме экзамена и включает 2 этапа: портфолио и экзамен. 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.

Экзамен проводится в устной форме. Во время проведения экзамена студенту разрешается использовать справочники, калькуляторы. В процессе ответа на вопросы экзаменационного билета 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
Семестр 7			
1	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или нескольких учебных дисциплинах.	Требования к структуре и содержанию портфолио
2	Экзаменационный билет	Комплекс вопросов.	Список теоретических вопросов

2.1 **Требования к структуре и содержанию оценочных средств аттестации**

2.1.1 Требования к структуре и содержанию портфолио
Портфолио должно содержать результаты выполнения 6 домашних заданий, состоящих из решения задач.
2.1.2 Форма и перечень вопросов экзаменационного билета

Форма экзаменационного билета

Таблица П1.3

Новосибирский государственный университет
Экзамен

Криптография для информационных технологий
наименование дисциплины

09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Программная инженерия и компьютерные науки
наименование образовательной программы

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №

1. Вопрос из категории 1
2. Вопрос из категории 2

Составитель

_____ Б.Я. Рябко
(подпись)

Ответственный за образовательную программу

_____ А.А. Романенко
(подпись)

«____»_____20 г.

Перечень вопросов экзамена, структурированный по категориям, представлен в таблице П1.4

Таблица П1.4

Категория	Формулировка вопроса
ПКС-2.3 Категория 1	Вопрос 1. Арифметика в конечных кольцах целых чисел..
	Вопрос 2. Алгоритмы возведения в степень.
	Вопрос 3. Алгоритмы вычисления мультипликативной инверсии.
ПКС-2.3 Категория 2	Вопрос 5. Понятие односторонней функции.
	Вопрос 6. Система Диффи-Хеллмана в мультипликативной группе.
	Вопрос 7. Система Диффи-Хеллмана в подгруппе простого поля
	Вопрос 8. Шифр Эль-Гамаля в мультипликативной группе
	Вопрос 9. Шифр Эль-Гамаля в подгруппе простого поля
	Вопрос 10. Шифр Шамира
	Вопрос 11. Вычисление дискретных логарифмов
	Вопрос 12. Извлечение корней в конечных кольцах целых чисел
	Вопрос 13. Шифр RSA
	Вопрос 14. Цифровая подпись RSA
	Вопрос 15. Шифр Рабина
	Вопрос 16. Стойкость систем RSA и Рабина
	Вопрос 17. Разложение числа на простые множители
	Вопрос 18. Доказательства с нулевым разглашением
	Вопрос 19. Протоколы аутентификации
ПКС-2.3 Категория 1	Вопрос 20. Электронные деньги
	Вопрос 21. Совершенные шифры
	Вопрос 22. Идеальные и строго идеальные шифры
	Вопрос 23. Рандомизация в криптографии
ПКС-2.3 Категория 2	Вопрос 24. Защита информации на основе нумерации.
	Вопрос 25. Омофонные коды
	Вопрос 26. Универсальное омофонное кодирование.

Набор экзаменационных билетов формируется и утверждается в установленном порядке в начале учебного года при наличии контингента обучающихся, завершающих освоение дисциплины «Криптография для информационных технологий» 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 (2 балла)	Пороговый уровень (3 балла)	Базовый уровень (4 балла)	Продвинутый (5 баллов)
ПКС-2.3	Портфолио	**ПКС-2.3** Уметь применять знания в области разработки ПО в предметной области	Фрагментарные знания	Знает как на основе основных функций и возможностей программного обеспечения проектировать и разрабатывать программные средства для систем защиты информации, но затрудняется при их использовании	Знает как на основе основных функций и возможностей программного обеспечения проектировать и разрабатывать программные средства для систем защиты информации, но с небольшими пробелами	Знает как на основе основных функций и возможностей программного обеспечения проектировать и разрабатывать программные средства для систем защиты информации исленного эксперимента
ПКС-2.3	Экзамен	**ПКС-2.3** Уметь применять знания в области разработки ПО в предметной области	Имеет фрагментарные знания методов исследования и проведения экспериментальных работ	Знать основные этапы проведения эксперимента с криптографическими методами.	Знать основные этапы проведения эксперимента с криптографическими методами. Но с пробелами.	Уметь проводить эксперименты с криптографическими методами по заданной методике и анализировать результатыУметь

4. Критерии выставления оценок по результатам промежуточной аттестации по дисциплине

В 7 семестре 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.

Лист актуализации фонда оценочных средств
промежуточной аттестации по дисциплине
«Криптография для информационных технологий»

№	Характеристика внесенных изменений (с указанием пунктов документа)	Дата и № протокола Ученого совета ФИТ	Подпись ответственного
1.	Актуализирован на 2020-2021 уч.год	22.07.2020 №77