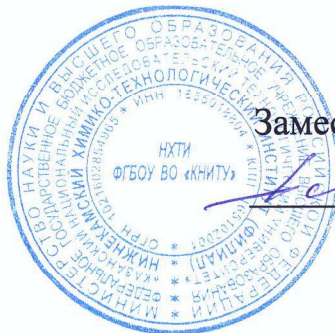



Министерство науки и высшего образования Российской Федерации  
Нижекамский химико-технологический институт (филиал)  
федерального государственного бюджетного образовательного учреждения  
высшего образования  
«Казанский национальный исследовательский технологический университет»  
(НХТИ ФГБОУ ВО «КНИТУ»)



УТВЕРЖДАЮ

Заместитель директора по УР

 Н.И. Никифорова  
« 30 » мая 2022 г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**

по дисциплине (модулю)

**Б1.В.10 Криптографические методы защиты информации**

(наименование дисциплины (модуля))

**09.03.02 «Информационные системы и технологии»**

(код и наименование направления подготовки/ специальности)

**Системы информационной безопасности**

(наименование профиля/программы/направленности/специализации)

*бакалавр*

квалификация

очная

форма обучения

Нижекамск, 2022 г.

Составитель ФОС:

доцент

(должность)

  
(подпись)

Л.Р. Вотякова

(Ф.И.О)

ФОС рассмотрен и одобрен на заседании кафедры ИСТ,  
протокол от 20.04.2022 г. № 8

Зав. кафедрой

  
(подпись)

О.В. Матухина

(Ф.И.О.)

Эксперт:

Руководитель ООП

Ф.И.О., должность, организация, подпись

  
Л.Р. Вотякова

**Перечень компетенций и индикаторов достижения компетенций с указанием этапов формирования в процессе освоения дисциплины**

Компетенция:

ПК-2 Способен обеспечить информационную безопасность на уровне баз данных

ПК-2.1 Знает угрозы безопасности баз данных, способы предотвращения

ПК-2.2 Умеет выявлять угрозы безопасности на уровне баз данных

ПК-2.3 Владеет навыками применения способов предотвращения угроз безопасности на уровне баз данных

<b>Индикаторы достижения компетенции</b>	<b>Этапы формирования в процессе освоения дисциплины</b> (указать все темы из РПД)				<b>Наименование оценочного средства</b>
	<b>Лекции</b>	<b>Практические Занятия</b>	<b>Лабораторные занятия</b>	<b>Курсовой проект (работа)</b>	
ПК-2.1, ПК-2.2, ПК-2.3	Тема 1-5	Не предусмотрены	Тема 1-5	Не предусмотрены	Выполнение лабораторной работы, вопросы к зачету

***Перечень оценочных средств по дисциплине (модулю)***

***Очная форма***

<b>№</b>	<b>Оценочные средства</b>	<b><i>Min, баллов (базовый уровень)</i></b>	<b><i>Max, баллов (повышенный уровень)</i></b>
1	Лабораторная работа №1	7	12
2	Лабораторная работа №2	7	12
3	Лабораторная работа №3	7	12
4	Лабораторная работа №4	7	12
5	Лабораторная работа №5	8	12
	<b>Текущий рейтинг</b>	<b>36</b>	<b>60</b>
	<b>Сдача зачета</b>	<b>24</b>	<b>40</b>
	<b>Рейтинг по дисциплине</b>	<b>60</b>	<b>100</b>

### ***Шкала оценивания***

<b>Выражение в баллах:</b>	<b>Словесное выражение</b>	<b>Критерии оценки индикаторов достижения при форме контроля:</b>
		<b>зачет</b>
60 - 100	зачтено	Оценка «зачтено» выставляется студенту, если ответы на вопросы по темам дисциплины последовательны, логически изложены, допускаются незначительные недочеты в ответе студента, такие как отсутствие самостоятельного вывода, речевые ошибки и пр
Ниже 60	незачтено	Оценка «не зачтено» выставляется студенту, если студент не знает основных понятий темы дисциплины, не отвечает на дополнительные и наводящие вопросы преподавателя.

### Краткая характеристика оценочных средства

<i>№ п/п</i>	<i>Наименование оценочного средства</i>	<i>Краткая характеристика оценочного средства</i>	<i>Представление оценочного сред- ства в фонде</i>
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>
1.	Лабораторная работа	<p>Это вид учебной работы, целью которой является изучение (исследование, измерение) характеристик лабораторного объекта.</p> <p>Цель лабораторных занятий: освоение изучаемой учебной дисциплины; приобретение навыков практического применения знаний учебной дисциплины (дисциплин) с использованием технических средств и (или) оборудования</p>	Темы лабораторных работ, контрольные вопросы по теме лабораторной работы

Министерство науки и высшего образования Российской Федерации  
Нижекамский химико-технологический институт (филиал)  
федерального государственного бюджетного образовательного учреждения  
высшего образования  
«Казанский национальный исследовательский технологический университет»

*Факультет Информационных технологий*  
*Кафедра Информационных систем и технологий*

Направление подготовки: 09.03.02 Информационные системы и технологии  
(код и наименование)

Профиль: Системы информационной безопасности

Учебным планом по направлению подготовки 09.03.02 Информационные системы и технологии для обучающихся предусмотрено проведение лабораторных занятий по дисциплине Б1.В.10 Криптографические методы защиты информации.

Лабораторные занятия по дисциплине проводятся в специально оборудованных лабораториях с применением необходимых средств обучения: лабораторного оборудования–персональных компьютеров, образцов для исследований, методических пособий. Цель проведения лабораторных работ – практическое освоение теоретических положений лекционного материала, а также выработка студентами определенных умений и навыков самостоятельного экспериментирования.

**Лабораторная работа №1.** Использование классических криптоалгоритмов подстановки и перестановки для защиты тексто-вой информации

Теоретические вопросы для подготовки к лабораторной работе

1. Какие вы знаете методы криптографической защиты файлов?
2. В чем преимущества и недостатки одноалфавитных методов?
3. Если необходимо зашифровать текст, содержащий важную информацию, какой метод из рассмотренных вы выберете? Обоснуйте свой выбор
4. Целесообразно ли повторно применять для уже зашифрованного текста:
  - а) метод многоалфавитного шифрования;
  - б) метод Цезаря? блоков

**Лабораторная работа №2.** Криптоанализ шифра простой замены

Теоретические вопросы для подготовки к лабораторной работе

1. Что такое энтропия языка?
2. Что понимается под избыточностью сообщения?
3. Что такое шифр простой замены?
4. В чем состоит обобщение шифра Цезаря?
5. Опишите краткую историю возникновения шифра Цезаря.
6. Объясните принцип дешифрования шифра простой замены.
7. Объяснить, почему при вскрытии шифра простой замены используется не полное ранжирование по частоте всех символов русского языка, а лишь 3-4 наиболее частых символов, как в п. 1.4?

8. Какими характеристиками должен обладать шифр, чтобы была возможность применить метод частотного анализа?
9. Какие виды криптоанализа Вам известны?
10. Охарактеризуйте базовую модель криптографии.
11. Какие основные разновидности шифров простой замены применялись в прошлом?
12. Сформулируйте правила шифрования/дешифрования шифра Цезаря.

**Лабораторная работа №3. Шифрование данных метода-миподстановки, перестановки и полиалфавитными шифрами**

Теоретические вопросы для подготовки к лабораторной работе

1. Почему метод подстановки имеет слабую надежность?
2. Что такое частотный анализ?
3. Что является криптографическим ключом в методе перестановки?
4. Как связаны метод подстановки и многоалфавитные шифры?
5. В чем отличие криптографии от криптоанализа?
6. По какому признаку шифры делят на симметричные и асимметричные?

**Лабораторная работа №4. Шифры многобуквенной замены на примере шифра Хилла**

Теоретические вопросы для подготовки к лабораторной работе

1. Предположим, что шифр Хилла используется для зашифрования открытого текста, представленного в виде двоичной последовательности. Сколько ключей имеет такой шифр?
2. К какому виду шифров относится шифр Хилла: поточным или блочным, докажете правильность своих рассуждений.
3. Приведите сравнительный анализ шифра Хилла и шифра Плейфейера.
4. Дайте математическое определение обратной матрицы.
5. Что такое стойкость шифра?
6. Оцените стойкость шифра Хилла при наличии достаточного числа пар соответствия открытого и зашифрованного текстов.
7. Дайте характеристику шифру Хилла.
8. В каких современных шифрах применяются идеи, подобные шифру Хилла?
9. Перечислите недостатки шифра Хилла

**Лабораторная работа №5. Шифр гаммирования**

Теоретические вопросы для подготовки к лабораторной работе

1. Какие параметры конгруэнтного генератора необходимо выбрать для получения максимальной длины последовательности псевдослучайных чисел?
2. От чего зависит длина псевдослучайной последовательности?
3. Каков принцип действия генераторов с обратной связью?
4. Какую операцию используют для шифрования в методе гаммирования?
5. Каковы достоинства и недостатки метода гаммирования?
6. Что является ключом в шифрах гаммирования?

Материалы лабораторных работ приведены в электронной информационно-образовательной среде ЭИОС НХТИ ФГБОУ ВО "КНИТУ": <https://moodle.nchti.ru/>.



Каждая инструкция содержит краткие теоретические сведения, относящиеся к данной работе, перечень необходимого оборудования, порядок выполнения работы, контрольные вопросы.

### **Критерии оценки лабораторных работ**

При подготовке к лабораторной работе по дисциплине Б1.В.10 Криптографические методы защиты информации в 6 семестре студент должен выполнить следующие виды работ:

<b>Виды работ</b>	<b>Минимальный балл</b>	<b>Максимальный балл</b>
Самостоятельная проработка теоретического материала к лабораторной работе	0	1
Ознакомление с установкой, ПК, методикой выполнения лабораторной работы	1	2
Выполнение необходимого эксперимента	2	3
Обработка результатов исследования, построение графиков	2	3
Анализ результатов исследования и вывод по работе	2	3
<b>ИТОГО :</b>	<b>7</b>	<b>12</b>

Таким образом, каждая лабораторная работа оценивается минимум в 7 баллов, максимум в 12 баллов. После выполнения всех работ рассчитывается итоговый балл по данному оценочному средству, как сумма по всем лабораторным работам.

Министерство науки и высшего образования Российской Федерации  
Нижекамский химико-технологический институт (филиал)  
федерального государственного бюджетного образовательного учреждения  
высшего образования  
«Казанский национальный исследовательский технологический университет»

*Факультет Информационных технологий*

*Кафедра Информационных систем и технологий*

Направление подготовки: 09.03.02 Информационные системы и технологии

Профиль: Системы информационной безопасности

Семестр 6

УТВЕРЖДАЮ

Зав. кафедрой

  
(подпись)

О.В.Матухина

« 20 \_ » \_\_04 2022 г

### **Вопросы к зачету**

**по дисциплине(модулю) Б1.В.10 Криптографические методы защиты информации**

1. Операции над множествами.
2. Бинарные отношения на множестве
3. Бинарные операции на множестве.
4. Алгебраические структуры.
5. Криптография. Конфиденциальность. Целостность. Аутентификация. Цифровая подпись.
6. Математическая модель шифра простой замены.
7. Элементы криптоанализа шифров перестановки.
8. Элементы криптоанализа поточного шифра простой замены.
9. Блочные шифры простой замены.
10. Многоалфавитные шифры замены.
11. Многоалфавитные шифры замены.
12. Повторное использование гаммы.
13. Элементы криптоанализа шифра Виженера.

### **Критерии оценки**

**Зачтено (24-40 б.):** выставляется, если обучающийся показывает всесторонние и глубокие знания программного материала, знание основной и дополнительной литературы; последовательно и четко отвечает на вопросы билета и дополнительные вопросы; уверенно ориентируется в проблемных ситуациях; демонстрирует способность применять теоретические знания для анализа практических ситуаций, делать правильные выводы, проявляет творческие способности в понимании, изложении и использовании программного материала; под-

тверждает полное освоение компетенций, предусмотренных программой.

**Незачтено (1-23 б):**выставляется, если обучающийся имеет существенные пробелы в знаниях основного учебного материала по разделу; не способен аргументированно и последовательно его излагать, допускает грубые ошибки в ответах, неправильно отвечает на задаваемые преподавателем вопросы или затрудняется с ответом; не подтверждает освоение компетенций, предусмотренных программой.