

Министерство науки и высшего образования Российской Федерации  
Бугульминский филиал федерального государственного бюджетного  
образовательного учреждения высшего образования  
«Казанский национальный исследовательский технологический университет»  
(БФ ФГБОУ ВО «КНИТУ»)

УТВЕРЖДАЮ  
Директор БФ ФГБОУ ВО «КНИТУ»  
Р.Ф.Хамидуллин  
« 04 » 06 2021г

### РАБОЧАЯ ПРОГРАММА

По дисциплине «Информационная безопасность и защита информации»  
Направление подготовки 09.03.02 «Информационные системы и технологии»  
Профиль/специализация Информационные системы и технологии  
Квалификация выпускника БАКАЛАВР  
Форма обучения очная/заочная  
Институт, факультет БФ ФГБОУ ВО «КНИТУ»  
Кафедра-разработчик рабочей программы МГД  
Курс, семестр очная форма 3 курс, 6 семестр  
Курс, семестр заочная форма 4 курс, 8 семестр

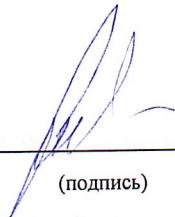
	часы (очная форма обучения)	Зачетные единицы	часы (заочная форма обучения)	Зачетные единицы
Лекции	27	0,75	6	0,16
Лабораторные занятия	54	1,5	12	0,33
Практические занятия				
Контроль самостоятельной работы	27	0,75	20	0,55
Самостоятельная работа	45	1,25	133	3,69
Фо ма аттестации	Экзамен	0,75	Экзамен	0,27
Всего	180	5	180	5

Бугульма, 2021 г.

Рабочая программа составлена с учетом требований Федерального государственного образовательного стандарта высшего образования № 926 от 19.09.2017 г. по направлению 09.03.02 «Информационные системы и технологии» на основании учебного плана набора обучающихся 2021 года.

Разработчик программы:

ст. преподаватель кафедры МГД



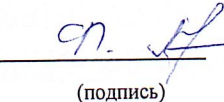
(подпись)

Лямов Ю.О.

(Ф.И.О)

Рабочая программа рассмотрена и одобрена на заседании кафедры МГД, протокол от 14.05 2021 г. № 10

Зав. кафедрой МГД, доцент



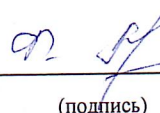
(подпись)

Ахмедзянова Ф.К.

(Ф.И.О)

**УТВЕРЖДЕНО**

Начальник УМО, доцент



(подпись)

Ахмедзянова Ф. К.

(Ф.И.О)

## **1. Цели освоения дисциплины**

Целями освоения дисциплины «Информационная безопасность и защита информации» являются:

- а) приобретение студентами необходимых теоретических знаний и практических навыков по обеспечению информационной безопасности компьютерных систем и сетей;
- б) изучение моделей управления доступом к информационным ресурсам компьютерных систем и способов защиты их от несанкционированного доступа;
- в) изучение криптографических методов защиты информации в компьютерных системах.

## **2. Место дисциплины в структуре основной образовательной программы**

Дисциплина «Информационная безопасность и защита информации» относится к формируемая участниками образовательных отношений части ООП и формирует у бакалавров по направлению подготовки 09.03.02 «Информационные системы и технологии» набор специальных знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Информационная безопасность и защита информации» бакалавр по направлению подготовки 09.03.02 «Информационные системы и технологии» должен освоить материал предшествующих дисциплин:

- 1) *Большие данные.*

Дисциплина «Информационная безопасность и защита информации» является предшествующей и необходима для успешного усвоения последующих дисциплин:

- 1) *Операционные системы;*
- 2) *Системное программное обеспечение.*

Знания, полученные при изучении дисциплины «Информационная безопасность и защита информации», могут быть использованы при прохождении учебной, производственной, преддипломной практики (в том числе научно-исследовательской работы), выполнении и защите выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

## **3. Компетенции и индикаторы достижения компетенции обучающегося, формируемые в результате освоения дисциплины:**

*ПК-2* Способен оценивать качество программного обеспечения, в том числе проведение тестирования и исследование результатов;

*ПК-2.1* Знает техники тестирования; основы работы в операционной системе; понимание среды применения разрабатываемого программного продукта;

*ПК-2.2* Умеет понимать процесс тестирования программного обеспечения и жизненный цикл программного продукта; проводить сравнительный анализ; сопоставлять и анализировать информацию;

*ПК-2.3* Владеет навыками выполнения необходимых видов тестирования в соответствии с планом тестирования; навыками анализа полученных результатов;

*ПК-3* Способен выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности;

*ПК-3.1* Знает основные приемы и нормы социального взаимодействия; принципы лидерства и формирования команды; технологии межличностной и групповой коммуникации в деловом взаимодействии;

*ПК-3.2* Умеет устанавливать и поддерживать контакты, обеспечивающие успешную работу в коллективе; применять основные методы и нормы социального взаимодействия для реализации своей роли и взаимодействия внутри команды;

*ПК-3.3* Владеет навыками социального взаимодействия и командной работы, распределения и реализации оптимальной роли в команде.

**В результате освоения дисциплины обучающийся должен:**

### **1) Знать:**

- а) общую постановку задачи обеспечения информационной безопасности компьютерных систем и сетей и классификацию методов ее решения;

- б) способы несанкционированного доступа к компьютерной информации и способы аутентификации пользователей;
- в) методы разграничения полномочий пользователей и управления доступом к ресурсам в защищенных операционных системах;
- г) способы построения симметричных и ассиметричных криптографических систем.

**2) Уметь:**

- а) применять методы разграничения полномочий пользователей и управления доступом к ресурсам в защищенных операционных системах;
- б) использовать методы и средства криптографической защиты информации;
- в) применять методы и средства защиты от вредоносных программ.

**3) Владеть:**

- а) освоить источники угроз к информационным системам;
- б) изучить модели защиты информационных систем;
- в) получить навыки для реализации различных моделей защиты компьютерных систем.

**4. Структура и содержание дисциплины «Информационная безопасность и защита информации»**

Общая трудоемкость дисциплины составляет для очной формы обучения 5 зачетных единиц, 180 часов; для заочной формы обучения 5 зачетных единиц, 180 часов.

Таблица 1а

Объем дисциплины (модуля) для очной формы обучения

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)					Оценочные средства для проведения промежуточной аттестации по разделам
			Лекции	Практические занятия	Лабораторные работы	СР	КСР	
1.	Комплексный подход к обеспечению информационной безопасности.	6	6	-	10	9	6	<i>Контрольная работа Лабораторная работа</i>
2.	Защита от несанкционированного доступа к информации в компьютерных системах.	6	4	-	10	9	4	<i>Лабораторная работа Доклад</i>
3.	Информационная безопасность и защита информации.	6	6	-	12	9	6	<i>Лабораторная работа Реферат</i>
4.	Компьютерные вирусы и механизмы борьбы с ними.	6	4	-	12	9	4	<i>Лабораторная работа Доклад</i>
5.	Защита от несанкционированного копирования информационных ресурсов.	6	7	-	10	9	7	<i>Лабораторная работа Доклад</i>
<b>ИТОГО</b>			<b>27</b>	<b>-</b>	<b>54</b>	<b>45</b>	<b>27</b>	
Форма аттестации			<i>Экзамен, 27 (часов)</i>					

## Объем дисциплины (модуля) для заочной формы обучения

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)					Оценочные средства для проведения промежуточной аттестации по разделам
			Лекции	Практические занятия	Лабораторные работы	КСР	СР	
1.	Комплексный подход к обеспечению информационной безопасности.	8	1	-	3	4	26	<i>Контрольная работа Лабораторная работа</i>
2.	Защита от несанкционированного доступа к информации в компьютерных системах.	8	1	-	3	4	25	<i>Лабораторная работа Доклад</i>
3.	Информационная безопасность и защита информации.	8	1	-	2	4	28	<i>Лабораторная работа Реферат</i>
4.	Компьютерные вирусы и механизмы борьбы с ними.	8	1	-	2	4	26	<i>Лабораторная работа Реферат</i>
5.	Защита от несанкционированного копирования информационных ресурсов.	8	2	-	2	4	28	<i>Лабораторная работа Реферат</i>
<b>ИТОГО</b>			<b>6</b>	<b>-</b>	<b>12</b>	<b>20</b>	<b>133</b>	
Форма аттестации			Экзамен, (9часов)					

## 5. Содержание лекционных занятий по темам (таблица 2 а – очная форма, таблица 2 б – заочная форма)

Таблица 2а

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Краткое содержание	Индикаторы достижения компетенции
1.	Комплексный подход к обеспечению информационной безопасности.	6	Основные понятия информационной безопасности. Угрозы безопасности информации и каналы утечки информации. Комплексный подход к защите информации. Организационная защита информации. Правовое обеспечение информационной безопасности. Инженерно-техническая, криптографическая и программно аппаратная защита информации.	Основные понятия информационной безопасности. Угрозы безопасности информации и каналы утечки информации. Комплексный подход к защите информации. Организационная защита информации. Правовое обеспечение информационной безопасности. Инженерно-техническая, криптографическая и программно аппаратная защита информации.	ПК-2; ПК-3
2.	Защита от несанкционированного доступа к информации в	4	Способы несанкционированного доступа к информации и защиты от	Способы несанкционированного доступа к информации и защиты от него. Способы аутентификации пользователей	ПК-2; ПК-3

	компьютерных системах.		него. Способы аутентификации пользователей компьютерных систем. Протокол ы аутентификации при удаленном доступе. Методы управления доступом к объектам компьютерных систем. Средства защиты информации в глобальных вычислительных сетях. Разграничение полномочий и управление доступом к ресурсам в защищенных версиях ОС Windows. Стандарт ы безопасности компьютерных систем и информационных технологий.	компьютерных систем. Протоколы аутентификации при удаленном доступе. Методы управления доступом к объектам компьютерных систем. Средства защиты информации в глобальных вычислительных сетях. Разграничение полномочий и управление доступом к ресурсам в защищенных версиях ОС Windows. Стандарты безопасности компьютерных систем и информационных технологий.	
3.	Информационная безопасность и защита информации.	6	Классификация методов криптографического преобразования информации Шифрование. Основные понятия. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом. Стандарты шифрования. Абсолютно стойкий шифр. Электронная цифровая подпись и ее использование. Функции хеширования. Принципы использования криптографического интерфейса ОС Windows. Компьютерная стеганография и его применения.	Классификация методов криптографического преобразования информации Шифрование. Основные понятия. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом. Стандарты шифрования. Абсолютно стойкий шифр. Электронная цифровая подпись и ее использование. Функции хеширования. Принципы использования криптографического интерфейса ОС Windows. Компьютерная стеганография и ее применение.	ПК-2; ПК-3
4.	Компьютерные вирусы и механизмы борьбы с ними.	4	Классификация компьютерных вирусов. Файловые вирусы. Загрузочные вирусы. Вирусы и операционные системы. Методы и средства борьбы с вирусами. Профилактика заражения вирусами компьютерных систем. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами.	Классификация компьютерных вирусов. Файловые вирусы. Загрузочные вирусы. Вирусы и операционные системы. Методы и средства борьбы с вирусами. Профилактика заражения вирусами компьютерных систем. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами.	ПК-2; ПК-3
5.	Защита от несанкционированного копирования информационных ресурсов.	7	Принципы построения и состав систем защиты от несанкционированного копирования. Методы защиты от копирования инсталляционных дисков и установленного программного обеспечения.	Принципы построения и состав систем защиты от несанкционированного копирования. Методы защиты от копирования инсталляционных дисков и установленного программного обеспечения.	ПК-2; ПК-3

Таблица 2б

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Краткое содержание	Индикаторы достижения компетенции
1.	Комплексный подход к обеспечению информационной безопасности.	1	Основные понятия информационной безопасности. Угрозы безопасности информации и каналы утечки информации. Комплексный подход к защите информации. Организационная защита информации. Правовое обеспечение информационной безопасности. Инженерно-техническая, криптографическая и программно аппаратная защита информации.	Основные понятия информационной безопасности. Угрозы безопасности информации и каналы утечки информации. Комплексный подход к защите информации. Организационная защита информации. Правовое обеспечение информационной безопасности. Инженерно-техническая, криптографическая и программно аппаратная защита информации.	ПК-2; ПК-3
2.	Защита от несанкционированного доступа к информации в компьютерных системах.	1	Способы несанкционированного доступа к информации и защиты от него. Способы аутентификации пользователей компьютерных систем. Протоколы аутентификации при удаленном доступе. Методы управления доступом к объектам компьютерных систем. Средства защиты информации в глобальных вычислительных сетях. Разграничение полномочий и управление доступом к ресурсам в защищенных версиях ОС Windows. Стандарты безопасности компьютерных систем и информационных технологий.	Способы несанкционированного доступа к информации и защиты от него. Способы аутентификации пользователей компьютерных систем. Протоколы аутентификации при удаленном доступе. Методы управления доступом к объектам компьютерных систем. Средства защиты информации в глобальных вычислительных сетях. Разграничение полномочий и управление доступом к ресурсам в защищенных версиях ОС Windows. Стандарты безопасности компьютерных систем и информационных технологий.	ПК-2; ПК-3
3.	Информационная безопасность и защита информации.	1	Классификация методов криптографического преобразования информации Шифрование. Основные понятия. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом. Стандарты шифрования. Абсолютно стойкий шифр. Электронная цифровая подпись и ее использование. Функции хеширования. Принципы использования криптографического интерфейса ОС	Классификация методов криптографического преобразования информации Шифрование. Основные понятия. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом. Стандарты шифрования. Абсолютно стойкий шифр. Электронная цифровая подпись и ее использование. Функции хеширования. Принципы использования криптографического интерфейса ОС Windows. Компьютерная стеганография и ее применение.	ПК-2; ПК-3

			Windows. Компьютерная стеганография и его применения.		
4.	Компьютерные вирусы и механизмы борьбы с ними.	1	Классификация компьютерных вирусов. Файловые вирусы. Загрузочные вирусы. Вирусы и операционные системы. Методы и средства борьбы с вирусами. Профилактика заражения вирусами компьютерных систем. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами.	Классификация компьютерных вирусов. Файловые вирусы. Загрузочные вирусы. Вирусы и операционные системы. Методы и средства борьбы с вирусами. Профилактика заражения вирусами компьютерных систем. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами.	ПК-2; ПК-3
5.	Защита от несанкционированного копирования информационных ресурсов.	2	Принципы построения и состав систем защиты от несанкционированного копирования. Методы защиты от копирования инсталляционных дисков и установленного программного обеспечения.	Принципы построения и состав систем защиты от несанкционированного копирования. Методы защиты от копирования инсталляционных дисков и установленного программного обеспечения.	ПК-2; ПК-3

### 6. Содержание практических занятий

Учебным планом направления 09.03.02 проведение практических занятий по дисциплине «Информационная безопасность и защита информации» не предусмотрено.

### 7. Содержание лабораторных занятий

Лабораторные работы проводятся в помещении учебной лаборатории.

Выполнение лабораторных работ проводится с целью систематизации и закрепления полученных теоретических знаний и практических умений по учебной дисциплине; углубления теоретических знаний в соответствии с заданной темой; формирования умений применять теоретические знания при решении поставленных вопросов; формированию компетенций.

Таблица 3а

№ п/п	Раздел дисциплины	Часы	Наименование лабораторной работы	Индикаторы достижения компетенции
1.	Комплексный подход к обеспечению информационной безопасности.	10	1.Тема: Комплексная защита и информационной системы	ПК-2; ПК-3; ПК-3.1; ПК-3.2
2.	Защита от несанкционированного доступа к информации в компьютерных системах.	10	1.Тема: Защита от несанкционированного доступа к информации в компьютерных системах.	ПК-2; ПК-3; ПК-3.1; ПК-3.2
3.	Информационная безопасность и защита информации.	12	1.Тема: Информационная безопасность и защита информации.	ПК-2; ПК-3; ПК-3.1; ПК-3.2
4.	Компьютерные вирусы и механизмы борьбы с ними.	12	1.Тема: Компьютерные вирусы и механизмы борьбы с ними.	ПК-2; ПК-3; ПК-3.1; ПК-3.2
5.	Создание анимации. Добавление звука в анимацию.	10	1.Тема: Защита от несанкционированного копирования информационных ресурсов. 2.Тема: Комплексная защита информационной системы.	ПК-2; ПК-3; ПК-3.1; ПК-3.2



Таблица 3б

№ п/п	Раздел дисциплины	Часы	Наименование лабораторной работы	Индикаторы достижения компетенции
1.	Комплексный подход к обеспечению информационной безопасности.	3	1.Тема: Комплексная защита и информационной системы	ПК-2; ПК-3; ПК-3.1; ПК-3.2
2.	Защита от несанкционированного доступа к информации в компьютерных системах.	3	1.Тема: Защита от несанкционированного доступа к информации в компьютерных системах.	ПК-2; ПК-3; ПК-3.1; ПК-3.2
3.	Информационная безопасность и защита информации.	2	1.Тема: Информационная безопасность и защита информации.	ПК-2; ПК-3; ПК-3.1; ПК-3.2
4.	Компьютерные вирусы и механизмы борьбы с ними.	2	1.Тема: Компьютерные вирусы и механизмы борьбы с ними.	ПК-2; ПК-3; ПК-3.1; ПК-3.2
5.	Создание анимации. Добавление звука в анимацию.	2	1.Тема: Защита от несанкционированного копирования информационных ресурсов. 2.Тема: Комплексная защита информационной системы.	ПК-2; ПК-3; ПК-3.1; ПК-3.2

8. Самостоятельная работа (таблица 4а – очная форма, таблица 4б – заочная форма)

Таблица 4а

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1.	Комплексный подход к обеспечению информационной безопасности.	9	Изучение лекционного материала и рекомендуемой литературы; подготовка к лабораторным работам	ПК-2; ПК-3; ПК-3.1; ПК-3.2
2.	Защита от несанкционированного доступа к информации в компьютерных системах	9	Изучение лекционного материала и рекомендуемой литературы; подготовка к лабораторным работам	ПК-2; ПК-3; ПК-3.1; ПК-3.2
3.	Информационная безопасность и защита информации	9	Изучение лекционного материала и рекомендуемой литературы; подготовка к лабораторным работам	ПК-2; ПК-3; ПК-3.1; ПК-3.2
4.	Компьютерные вирусы и механизмы борьбы с ними	9	Изучение лекционного материала и рекомендуемой литературы; подготовка к лабораторным работам	ПК-2; ПК-3; ПК-3.1; ПК-3.2
5.	Защита от несанкционированного копирования информационных ресурсов.	9	Изучение лекционного материала и рекомендуемой литературы; подготовка к лабораторным работам.	ПК-2; ПК-3; ПК-3.1; ПК-3.2

Таблица 4б

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1.	Комплексный подход к обеспечению информационной безопасности.	26	Изучение лекционного материала и рекомендуемой литературы; подготовка к лабораторным работам.	ПК-2; ПК-3; ПК-3.1; ПК-3.2
2.	Защита от несанкционированного доступа к информации в компьютерных системах.	25	Изучение лекционного материала и рекомендуемой литературы; подготовка к лабораторным работам.	ПК-2; ПК-3; ПК-3.1; ПК-3.2
3.	Информационная безопасность и защита информации.	28	Изучение лекционного материала и рекомендуемой литературы;	ПК-2; ПК-3; ПК-3.1;

			подготовка к лабораторным работам.	ПК-3.2
4.	Компьютерные вирусы и механизмы борьбы с ними.	26	Изучение лекционного материала и рекомендуемой литературы; подготовка к лабораторным работам.	ПК-2; ПК-3; ПК-3.1; ПК-3.2
5.	Защита от несанкционированного копирования информационных ресурсов.	28	Изучение лекционного материала и рекомендуемой литературы; подготовка к лабораторным работам.	ПК-2; ПК-3; ПК-3.1; ПК-3.2

**8.1 Контроль самостоятельной работы** (таблица 5а – очная форма, таблица 5б – заочная форма)

Таблица 5а

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1.	Правовое обеспечение информационной безопасности. Основные понятия информационной безопасности.	6	Прием лабораторных работ. Консультирование. Проверка доклада	ПК-2, ПК-2.1; ПК-2.2; ПК-2.3; ПК-3, ПК-3.1, ПК-3.2; ПК-3.3
2.	Средства защиты информации в глобальных вычислительных сетях. Стандарты безопасности компьютерных систем и информационных технологий.	4	Прием лабораторных работ. Консультирование. Проверка доклада	ПК-2, ПК-2.1; ПК-2.2; ПК-2.3; ПК-3, ПК-3.1, ПК-3.2; ПК-3.3
3.	Принципы использования криптографического интерфейса ОС Windows.	6	Прием лабораторных работ. Консультирование. Проверка реферата	ПК-2, ПК-2.1; ПК-2.2; ПК-2.3; ПК-3, ПК-3.1, ПК-3.2; ПК-3.3
4.	Профилактика заражения вирусами компьютерных систем. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами.	4	Прием лабораторных работ. Консультирование.	ПК-2, ПК-2.1; ПК-2.2; ПК-2.3; ПК-3, ПК-3.1, ПК-3.2; ПК-3.3
5.	Методы защиты от копирования инсталляционных дисков и установленного программного обеспечения.	7	Прием лабораторных работ. Консультирование. Проверка реферата	ПК-2, ПК-2.1; ПК-2.2; ПК-2.3; ПК-3, ПК-3.1, ПК-3.2; ПК-3.3

Таблица 5б

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1.	Правовое обеспечение информационной безопасности. Основные понятия информационной безопасности.	4	Прием лабораторных работ. Консультирование. Проверка контрольной работы	ПК-2, ПК-2.1; ПК-2.2; ПК-2.3; ПК-3, ПК-3.1, ПК-3.2; ПК-3.3
2.	Средства защиты информации в глобальных вычислительных сетях. Стандарты безопасности компьютерных систем и информационных технологий.	4	Прием лабораторных работ. Консультирование.	ПК-2, ПК-2.1; ПК-2.2; ПК-2.3; ПК-3, ПК-3.1, ПК-3.2; ПК-3.3
3.	Принципы использования криптографического интерфейса ОС Windows.	4	Прием лабораторных работ. Консультирование.	ПК-2, ПК-2.1; ПК-2.2; ПК-2.3; ПК-3, ПК-3.1, ПК-3.2; ПК-3.3

4.	Профилактика заражения вирусами компьютерных систем. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами.	4	Прием лабораторных работ. Консультирование.	ПК-2, ПК-2.1; ПК-2.2; ПК-2.3; ПК-3, ПК-3.1, ПК-3.2; ПК-3.33
5.	Методы защиты от копирования инсталляционных дисков и установленного программного обеспечения.	4	Прием лабораторных работ. Консультирование. Проверка реферата	ПК-2, ПК-2.1; ПК-2.2; ПК-2.3; ПК-3, ПК-3.1, ПК-3.2; ПК-3.3

### 9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности студентов в рамках дисциплины «Информационная безопасность и защита информации» используется рейтинговая система. Рейтинговая оценка формируется на основании текущего и промежуточного контроля. Максимальное и минимальное количество баллов по различным видам учебной работы описано в «Положении о балльно-рейтинговой системе оценки знаний студентов и обеспечения качества учебного процесса» ФГБОУ ВО «КНИТУ».

При изучении указанной дисциплины предусматривается выполнение лабораторных работ, тестирования, реферата и расчетных работ. За эти контрольные точки студент может получить минимальное и максимальное количество баллов (см. таблицу). За Экзамен студент может получить максимальное количество баллов – 5. В итоге максимальный рейтинг за изучение дисциплины составляет 100 баллов (таблица 6).

Таблица 6

Оценочные средства	Кол-во	Min, баллов	Max, баллов
Лабораторная работа	4	27	35
Доклад	-	-	-
Реферат	-	9	15
Контрольная работа	-	24	50
Экзамен	1	60	100
<b>Итого</b>			

### 10. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Оценочные средства для проведения текущего контроля успеваемости, промежуточной аттестации обучающихся и итоговой (государственной итоговой) аттестации разрабатываются согласно положению о Фондах оценочных средств, рассматриваются как составная часть рабочей программы и оформляются отдельным документом.

### 11. Информационно-методическое обеспечение дисциплины

#### 11.1. Основная литература

При изучении дисциплины «Информационная безопасность и защита информации» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Кол-во экз.
1. Ищейнов В. Я. Информационная безопасность и защита информации: теория и практика: учебное пособие: [16+] / В. Я. Ищейнов. М.; Берлин: Директ-Медиа, 2020. 271 с.	ЭБС «Университетская библиотека ONLINE» <a href="http://www.biblioclub.ru">www. biblioclub.ru</a> . Режим доступа: по подписке. URL: Доступ с любой точки интернет после регистрации с IP-адресов КНИТУ
2. Введение в информационную безопасность и защиту информации учебное пособие: [16+] /	ЭБС «Университетская библиотека ONLINE» <a href="http://www. biblioclub.ru">www. biblioclub.ru</a> . Режим доступа: по подписке.

В. А. Трушин, Ю. А. Котов, Л. С. Левин, К. А. Донской. Новосибирск: Новосибирский государственный технический университет, 2017. 132 с.	URL: <a href="https://biblioclub.ru/index.php?page=book&amp;id=575113">https://biblioclub.ru/index.php?page=book&amp;id=575113</a> Доступ с любой точки интернет после регистрации с IP-адресов КНИТУ
---	--

### 11.2 Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Кол-во экз.
1. Основы информационной безопасности: учебное пособие для студентов вузов / Е. В. Вострцова. Екатеринбург: Изд-во Урал-ун-та, 2019. 204 с.	ЭБС «Университетская библиотека ONLINE» <a href="http://www.biblioclub.ru">www.biblioclub.ru</a> . Режим доступа: по подписке. URL <a href="https://biblioclub.ru/index.php?page=book&amp;id=493253">https://biblioclub.ru/index.php?page=book&amp;id=493253</a> Доступ с любой точки интернет после регистрации с IP-адресов КНИТУ

В том числе учебники, учебные пособия, учебно-методические пособия, учебно-методические указания, монографии, практикумы, тексты лекций, сборники конференций.

### 11.3 Электронные источники информации

При изучении дисциплины «Информационная безопасность и защита информации» в качестве электронных источников информации, рекомендуется использовать следующие источники:

При изучении дисциплины «Информационная безопасность и защита информации» в качестве электронных источников информации, рекомендуется использовать следующие источники:

Введение в информатику: Информация. [Электронный ресурс]. – Режим доступа: <http://www.intuit.ru/studies/courses/108/108/info>;

Научная Электронная Библиотека (НЭБ) – Режим доступа: <https://elibrary.ru/defaultx.asp>;

ЭБС «Лань» – Режим доступа: <https://e.lanbook.com/books/>;

ЭБС «Университетская Библиотека Онлайн» – Режим доступа: <https://biblioclub.ru/>;

ЭБС «Юрайт» – Режим доступа: <https://urait.ru/>.

Согласовано:

Библиотекарь

*Латыпова*

А.Г. Латыпова

### 11.4 Современные профессиональные базы данных и информационные справочные системы.

1. Виртуальная среда обучения КНИТУ - [https://moodle.kstu.ru/?id\\_e=68073](https://moodle.kstu.ru/?id_e=68073). Доступ по логину-пароллю регистрации в КНИТУ.

2. Единое окно доступа к образовательным ресурсам (раздел Инфокоммуникационные системы и сети и информационные технологии) [http://window.edu.ru/catalog/?p\\_rubr=2.2.75.6](http://window.edu.ru/catalog/?p_rubr=2.2.75.6). Доступ свободный.

3. Министерство науки и высшего образования Российской Федерации <https://minobrnauki.gov.ru/>. Доступ свободный.

4. Справочная правовая система КонсультантПлюс. Содержится огромный массив справочной правовой информации, российское и региональное законодательство, консультации для бюджетных организаций, комментарии законодательства, формы документов, проекты нормативных правовых актов, международные правовые акты, правовые акты, технические нормы и правила - <http://www.consultant.ru>

5. Электронные версии периодических изданий, размещенные на сайте информационных ресурсов [www.polpred.com](http://www.polpred.com).

### **12. Материально-техническое обеспечение дисциплины.**

Учебные аудитории для проведения учебных занятий оснащены оборудованием:

1. Учебные столы, стулья;
2. Доска;
3. Стол преподавателя;
4. Компьютерные столы, стулья;

Техническими средствами обучения:

1. Персональные компьютеры (с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду КНИТУ);

2. Сеть Интернет;
3. Мультимедиа-проектор.

Помещения для самостоятельной работы оснащены компьютерной техникой:

1. Персональный компьютер;
2. Столы компьютерные;
3. Учебные столы, стулья.

Лицензированное программное обеспечение и свободно распространяемое программное обеспечение, используемое в учебном процессе при освоении дисциплины «Информационная безопасность и защита информации»:

1. MOODLE – Виртуальная среда обучения КНИТУ;
2. MS Teams: <https://products.office.com/ru-ru/microsoft-teams/download-app>;
3. Управленческое ПО «Ваш финансовый аналитик 2: Сетевой»;
4. Управленческое ПО, 1С: Предприятие 8. Комплект для обучения в высших и средних учебных заведениях;
5. MS Office 2007 Russian (от 16.10.2008г. лицензия № 44684779);
6. MS Office 2007 Professional Russian (от 16.10.2008г. лицензия № 44684779),  
MS Win Home 10 64 Bin Russian (от 15.02. 2018);
7. MS Office Home and Student 2016 Bin Russian (от 15.02. 2018).

### **13. Образовательные технологии**

Количество занятий, проводимых в интерактивных формах.

Основные интерактивные формы проведения учебных занятий:

- творческие задания;
- работа в малых группах;
- дискуссия;
- обучающие игры (ролевые игры, имитации, деловые игры и образовательные игры);
- изучение и закрепление нового материала на интерактивной лекции (лекция-беседа, лекция – дискуссия, лекция с разбором конкретных ситуаций, лекция с заранее запланированными ошибками, лекция- пресс-конференция, мини-лекция);
- эвристическая беседа;
- разработка проекта (метод проектов);
- системы дистанционного обучения.

### Лист переутверждения рабочей программы

Рабочая программа по дисциплине «Информационная безопасность и защита информации».

По направлению 09.03.02 «Информационные системы и технологии»

для профиля «Информационные системы и технологии»

для набора обучающихся 2021 года.

пересмотрена на заседании кафедры Менеджмента и гуманитарных дисциплин

№ п/п	Дата переутверждения РП (протокол заседания кафедры №__ от __. __. 20__)	Наличие изменений	Наличие изменений в списке литературы	Подпись разработчика РП	Подпись заведующего кафедрой	Подпись начальника УМО