

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

«15» апреля 2023 г.

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 заочная
Институт, факультет БФ ФГБОУ ВО «КНИТУ»
Кафедра-разработчик рабочей программы МГД
Курс, семестр заочная форма 4 курс, 8 семестр

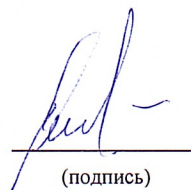
	Часы	Зачетные единицы
Лекции	6	0,16
Практические занятия	-	-
Лабораторные занятия	12	0,33
Контроль самостоятельной работы	20	0,55
Самостоятельная работа	133	3,7
Форма аттестации: экзамен	9	0,26
Всего	180	5

Бугульма, 2023

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 2023 года.

Разработчик программы:

ст. преподаватель кафедры МГД



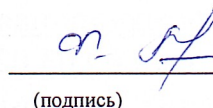
(подпись)

Лямов Ю.О.

(Ф.И.О.)

Рабочая программа рассмотрена и одобрена на заседании кафедры МГД, протокол от 21.04 2023 г. № 9

Зав. кафедрой МГД, доцент



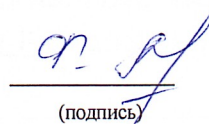
(подпись)

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 части, формируемой участниками образовательных отношений ООП и формирует у бакалавров по направлению подготовки 09.03.02 «Информационные системы и технологии» набор 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. *Дискретная математика*
2. *Информатика*
3. *Информационные технологии*
4. *Технологии программирования*

Дисциплина «Большие данные» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. *Введение в распределенные системы*
2. *Методы искусственного интеллекта*
3. *Управление информационными процессами*

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 теорию баз данных, основы программирования, возможности информационных систем, инструменты и методы проектирования структур баз данных;

ПК - 3.2 Умеет применять методы разграничения полномочий пользователей и управления доступом к ресурсам в защищенных операционных системах; разрабатывать структуру баз данных;

ПК - 3.3 Владеет моделями защиты информационных систем; навыками разработки структуры баз данных информационных систем в соответствии с архитектурной спецификацией.

В результате освоения дисциплины обучающийся должен:

Знать:

- методы разграничения полномочий пользователей и управления доступом к ресурсам в защищенных операционных системах;

- способы построения симметричных и асимметричных криптографических систем
- знать общую постановку задачи обеспечения информационной безопасности компьютерных систем и сетей и классификацию методов ее решения;

- способы несанкционированного доступа к компьютерной информации и способы аутентификации пользователей.

Уметь:

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

- использовать методы и средства криптографической защиты информации.

Владеть:

- изучить модели защиты информационных систем;
- получить навыки для реализации различных моделей защиты компьютерных систем;

- освоить источники угроз к информационным системам;

- изучить модели защиты информационных систем

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

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 180 часов.

Таблица 1

Объем дисциплины (модуля)

№ 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	-	2		24	<i>Лабораторная работа</i>
2.	Защита от несанкционированного доступа к информации в компьютерных системах	8	2	-	4	5	28	<i>Лабораторная работа</i>
3.	Информационная безопасность и защита информации	8	1	-	4	5	28	
4.	Компьютерные вирусы и механизмы борьбы с ними	8	1	-	1	5	28	
5.	Защита от несанкционированного копирования информационных ресурсов	8	1	-	1	5	25	<i>Лабораторная работа</i>
ИТОГО			6	-	12	20	133	
Форма аттестации								<i>Экзамен</i>

5. Содержание лекционных занятий по темам

Таблица 2

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1.	Комплексный подход к обеспечению информационной безопасности	1	Комплексный подход к обеспечению информационной безопасности	ПК-2.1; ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3

2.	Защита от несанкционированного доступа к информации в компьютерных системах	2	Защита от несанкционированного доступа к информации в компьютерных системах	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
3.	Информационная безопасность и защита информации	1	Информационная безопасность и защита информации	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
4.	Компьютерные вирусы и механизмы борьбы с ними	1	Компьютерные вирусы и механизмы борьбы с ними	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
5.	Защита от несанкционированного копирования информационных ресурсов	1	Защита от несанкционированного копирования информационных ресурсов	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
Всего		6		

6. Содержание семинарских, практических занятий

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

7. Содержание лабораторных занятий

Таблица 3

№ п/п	Раздел дисциплины	Часы	Наименование лабораторной работы	Индикаторы достижения компетенции
1	Комплексный подход к обеспечению информационной безопасности	2	Комплексный подход к обеспечению информационной безопасности	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
2	Защита от несанкционированного доступа к информации в компьютерных системах	4	Защита от несанкционированного доступа к информации в компьютерных системах	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
3	Информационная безопасность и защита информации	4	Компьютерные вирусы и механизмы борьбы с ними	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
4	Компьютерные вирусы и механизмы борьбы с ними	1	Защита от несанкционированного копирования информационных ресурсов	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
5	Защита от несанкционированного копирования информационных ресурсов	1	Компьютерные вирусы и механизмы борьбы с ними	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
Всего		12		

8. Самостоятельная работа

Таблица 4

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1.	Комплексный подход к обеспечению информационной безопасности	24	подготовка к лабораторной работе	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3

2.	Защита от несанкционированного доступа к информации в компьютерных системах	28	подготовка к лабораторной работе, подготовка к экзамену, проработка лекционного материала	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
3.	Информационная безопасность и защита информации	28	подготовка к лабораторной работе, подготовка к экзамену	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
4.	Компьютерные вирусы и механизмы борьбы с ними	28	подготовка к лабораторной работе, подготовка к экзамену, проработка лекционного материала	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
5.	Защита от несанкционированного копирования информационных ресурсов	25	подготовка к лабораторной работе, подготовка к экзамену, проработка лекционного материала	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
Всего		133		

8.1 Контроль самостоятельной работы

Таблица 5

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1.	Комплексный подход к обеспечению информационной безопасности	5	Прием лабораторной работы	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
2.	Защита от несанкционированного доступа к информации в компьютерных системах	5	Прием лабораторной работы	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
3.	Информационная безопасность и защита информации	5	Прием лабораторной работы	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
4.	Компьютерные вирусы и механизмы борьбы с ними	5	Прием лабораторной работы	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
5.	Защита от несанкционированного копирования информационных ресурсов	5	Прием лабораторной работы	ПК-2.1;ПК-2.2; ПК-2.3; ПК-3.1; ПК-3.2 ПК-3.3
Всего		20		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности, обучающихся в рамках дисциплины «Информационная безопасность и защита информации» используется рейтинговая система. 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. Рейтинговая оценка формируется на основании текущего и промежуточного контроля. За контрольные точки студент может получить минимальное и максимальное количество баллов (см. таблицу).

Таблица 6

Оценочные средства	Кол-во	Min, баллов	Max, баллов
8 семестр			
Лабораторная работа	6	36	60
Экзамен	1	24	40

Итого		60	100
--------------	--	-----------	------------

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	Количество экземпляров
1. Щеглов А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. Москва: Издательство Юрайт, 2023. 309 с. (Высшее образование).	ЭБС «Юрайт» https://www.urait.ru/bcode/511998 Доступ с любой точки интернет после регистрации с IP-адресов БФ КНИТУ
Зенков А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. 2-е изд., перераб. и доп. Москва: Издательство Юрайт, 2023. 107 с. (Высшее образование).	ЭБС «Юрайт» URL: https://www.urait.ru/bcode/530927 Доступ с любой точки интернет после регистрации с IP-адресов БФ КНИТУ
Суворова Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. 2-е изд., перераб. и доп. Москва: Издательство Юрайт, 2023. 277 с. (Высшее образование).	ЭБС «Юрайт» URL: https://www.urait.ru/bcode/531084 Доступ с любой точки интернет после регистрации с IP-адресов БФ КНИТУ

11.2 Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Кол-во экз.
1. Чернова Е. В. Информационная безопасность человека: учебное пособие для вузов / Е. В. Чернова. 3-е изд., перераб. и доп. Москва: Издательство Юрайт, 2023. — 327 с. (Высшее образование).	ЭБС «Юрайт» Режим доступа: по подписке. URL: URL: https://www.urait.ru/bcode/531682 Доступ с любой точки интернет после регистрации с IP-адресов БФ 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:

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

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

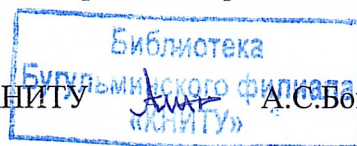
ЭБС «Юрайт» – Режим доступа: <https://urait.ru/>

ЭБС «Znanium.com» - Режим доступа: <https://znanium.com/>

ЭБС «IPR SMART» - Режим доступа: <https://www.iprbookshop.ru/>

Согласовано:

Библиотекарь БФ ФГБОУ ВО КНИТУ А.С. Боговик



11.4. Профессиональные базы данных и информационные справочные системы.

Базы данных Wiley Online Library: <https://onlinelibrary.wiley.com/>

Springer Nature: <https://link.springer.com/> zbMath: <https://zbmath.org/>

Информационные справочные системы:

Справочно-правовая система «ГАРАНТ» Доступ свободный: www.garant.ru

Справочно-правовая система «КонсультантПлюс» Доступ свободный: www.consultant.ru

Журнал «Системная информатика» https://www/system-informatics-ru/ru/research_area/raspredelennye-sistemy;

Журнал «Технологии защиты» <http://www/tzmagazine.ru/jpage.-php?uid1=378&uid2=471&uid3=484>

журнал «Parallel Computing» <https://www/journals.lsevier.com/parallel-computing>

12. Материально-техническое обеспечение дисциплины.

Учебные аудитории для проведения учебных занятий оснащены оборудованием: парты, стулья, доска; техническими средствами обучения: проектор, персональные компьютеры, с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду КНИТУ.

Помещения для самостоятельной работы оснащены компьютерной техникой: персональные компьютеры, с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду КНИТУ. с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду КНИТУ.

13. Образовательные технологии

Количество часов занятий, проводимых в интерактивных формах в учебном процессе по дисциплине «Информационная безопасность и защита информации» составляет 9 ч.

В процессе освоения дисциплины «Информационная безопасность и защита информации» используются следующие образовательные технологии:

- работа в малых группах;
- разработка проекта (метод проектов);

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» 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