МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное
образовательное учреждение высшего образования
«Казанский национальный исследовательский
технологический университет»
(ФГБОУ ВО «КНИТУ»)

УТВЕРЖДАЮ
Проректор по учебной работе
А.В. Бурмистров
«29» июня 2020 г.

Рабочая программа дисциплины в виде электронного документа выгружена из информационной системы управления университетом и соответствует оригиналу
Простая электронная подпись, ID подписи: 1020
Подписал Проректор по учебной работе А.В. Бурмистров
Дата 29.06.2020

РАБОЧАЯ ПРОГРАММА
по дисциплине **«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ»**

Направление подготовки:	09.03.02 Информационные системы и технологии
Профиль:	Информационные системы и технологии
Квалификация выпускника:	Бакалавр
Форма обучения:	Заочная
Институт:	Институт технологии легкой промышленности, моды и дизайна
Факультет:	Факультет дизайна и программной инженерии
Кафедра-разработчик:	Кафедра «Информатики и прикладной математики»
Курс; семестр	4; 11, 12

Вид нагрузки	Часы	Зачётные единицы
Лекция	8	0,22
Лабораторная работа	16	0,44
Контроль самостоятельной работы	20	0,56
Самостоятельная работа	127	3,53
Форма аттестации: Контрольная работа (12 сем), Экзамен (12 сем)	9	0,25
Всего	180	5

Казань, 2020

Рабочая программа составлена с учётом требований Федерального государственного образовательного стандарта (приказ № 926 от 19.09.2017) по направлению подготовки 09.03.02 Информационные системы и технологии для профиля «Информационные системы и технологии» на основании учебных планов набора обучающихся 2020 года.

Разработчик программы:

Доцент	В.А. Богомолов
Доцент	Е.А. Печеный

С О Г Л А С О В А Н О
Рабочая программа рассмотрена и одобрена на заседании кафедры «Информатики и прикладной математики», протокол от 11.05.2020 г. № 6.
Заведующий кафедрой ***Согласовано*** Н.К. Нуриев

У Т В Е Р Ж Д Е Н О
Начальник центра УМЦ ***Утверждаю*** Л.А. Китаева

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 образовательной программы

Дисциплина «Информационная безопасность и защита информации» относится к формируемой участниками образовательных отношений части ООП и формирует у обучающихся по профилю «Информационные системы и технологии» набор знаний, умений, навыков и компетенций.

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

1. Информатика
2. Технологии программирования

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

1. Корпоративные информационные системы
2. Моделирование физических процессов

3. 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:

- 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

- Методы разграничения полномочий пользователей и управления доступом к ресурсам в защищенных операционных системах.

- способы построения симметричных и асимметричных криптографических систем

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

Владеть:

- изучить модели защиты информационных систем;

- получить навыки для реализации различных моделей защиты компьютерных систем

освоить источники угроз к информационным системам

4. Структура и содержание дисциплины

Общая трудоёмкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Раздел дисциплины	Семе-стр	Виды учебной работы (в часах)					Оценочные средства для проведения текущей и промежу-точной аттестации
			Лекция	Практические занятия	Лабора-торные	КСР	СРС	
1	2	3	4	5	6	7	8	9
1.	Комплексный подход к обеспечению информационной безопасности	11	2					Контрольная работа
2.	Защита от несанкционированного доступа к информации в компьютерных системах	11					7	
	Итого по семестру	**11**	**2**				**7**	
1.	Информационная безопасность и защита информации	12	2		4	6	40	Контрольная работа; Лабораторная работа
2.	Компьютерные вирусы и механизмы борьбы с ними	12	2		4	6	40	
3.	Защита от несанкционированного копирования информационных ресурсов	12	2		8	8	40	Лабораторная работа; Экзамен
	Итого по семестру	**12**	**6**		**16**	**20**	**120**	**Контрольная работа, Экзамен**

5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Комплексный подход к обеспечению информационной безопасности	2	Основные понятия информационной безопасности. Угрозы безопасности информации и каналы утечки информации	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
2.	Информационная безопасность и защита информации	2	Способы несанкционированного доступа к информации и защиты от него	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
3.	Компьютерные вирусы и механизмы борьбы с ними	2	Шифрование. Основные понятия. Методы шифрования с симметричным ключом	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
4.	Защита от несанкционированного копирования информационных ресурсов	2	Принципы построения и состав систем защиты от несанкционированного копирования	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
	ВСЕГО	**8**		

6. Содержание практических/семинарских занятий

Проведение практических/семинарских занятий не предусмотрено учебным планом

7. Содержание лабораторных занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Информационная безопасность и защита информации	4	Комплексная защита информационной системы	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
2.	Компьютерные вирусы и механизмы борьбы с ними	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.	Защита от несанкционированного копирования информационных ресурсов	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.		4	Защита от несанкционированного копирования информационных ресурсов	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
	ВСЕГО	**16**		

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Комплексный подход к обеспечению информационной безопасности	7	подготовка к контрольной работе	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
2.	Информационная безопасность и защита информации	40	подготовка к контрольной работе, подготовка к лабораторной работе	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
3.	Компьютерные вирусы и механизмы борьбы с ними	40	подготовка к контрольной работе, подготовка к лабораторной работе	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
4.	Защита от несанкционированного копирования информационных ресурсов	40	подготовка к контрольной работе, подготовка к лабораторной работе	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
	ВСЕГО	**127**		

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Информационная безопасность и защита информации	6	прием лабораторной работы, проверка контрольной работы	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
2.	Компьютерные вирусы и механизмы борьбы с ними	6	прием лабораторной работы, проверка контрольной работы	ПК-2.1 ПК-2.2 ПК-2.3 ПК-3.1 ПК-3.2 ПК-3.3
3.	Защита от несанкционированного копирования информационных ресурсов	8	прием лабораторной работы, проверка контрольной 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).

Оценочные средства	Кол-во	Мин.баллов	Макс.баллов
12-й семестр			
Лабораторная работа	4	24	44
Экзамен	1	24	40
Контрольная работа	1	12	16
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 и 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
Э.Г. Дадян, Современные базы данных. Основы. Часть 1 [Прочее] Учебное пособие: Москва : ООО "Научно-издательский центр ИНФРА-М", 2017	http://znanium.com/go.php?id=959289 Режим доступа: по подписке КНИТУ
Н. В. Бессарабов, Модели и смыслы данных в Cache и Oracle [Электронный ресурс] : Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016	http://www.iprbookshop.ru/73652.html Режим доступа: по подписке КНИТУ

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Количество экземпляров
Э.Г. Дадян, Современные базы данных. Часть 2: практические задания [Прочее] Учебно-методическое пособие: Москва : ООО "Научно-издательский центр ИНФРА-М", 2017	http://znanium.com/go.php?id=959288 Режим доступа: по подписке КНИТУ

11.3. Электронные источники информации

При изучении дисциплины «Информационная безопасность и защита информации» предусмотрено использование электронных источников информации:

1. Электронный каталог УНИЦ КНИТУ: Режим доступа: http://ruslan.kstu.ru/
2. ЭБС «Лань»:Режим доступа: https://e.lanbook.com
3. Образовательная платформа «Юрайт»: Режим доступа: https://urait.ru/
4. ЭБС «Znanium.com»: Режим доступа: http://znanium.com/
5. ЭБС Университетская библиотека онлайн: Режим доступа: http://biblioclub.ru/

6. ЭБС IPRbooks: Режим доступа: http://www.iprbookshop.ru/
7. ЭБС BOOK.ru : Режим доступа: https://www.book.ru/
8. Научная электронная библиотека https://elibrary.ru/

11.4. Профессиональные базы данных и информационные справочные системы

Базы данных

Scopus Доступ свободный: www.scopus.com
Web of Science Доступ свободный: apps.webofknowledge.com

Информационные справочные системы

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

12. Материально-техническое обеспечение дисциплины

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

Офисные и деловые программы: ABBYY FineReader 9.0 проф;
Офисные и деловые программы: MS Office 2007 Russian;
Офисные и деловые программы: MS Office 2007 Professional Russian;
Офисные и деловые программы: MS Office 2010-2016 Standard
Архиватор 7 Zip
Блокнот Notepad
Яндекс Браузер

Пакет прикладных математических программ, предоставляющий открытое окружение для инженерных (технических) и научных расчётов Scilab 6.0.2.
Свободно распространяемая среда разработки Python
Свободно распространяемая база данных MySQL

Учебные аудитории Д-507а, Д 229 для проведения учебных занятий оснащены оборудованием:
парты,
стулья,
доска;

техническими средствами обучения:
проектор

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.

* Допускается замена оборудования его виртуальными аналогами.

13. Образовательные технологии

Количество часов занятий, проводимых в интерактивных формах в учебном процессе по дисциплине «Информационная безопасность и защита информации» составляет 6 ч.

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

• работа в малых группах;
• разработка проекта (метод проектов);
• системы дистанционного обучения