Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Казанский национальный исследовательский технологический университет»
(ФГБОУ ВО «КНИТУ»)

УТВЕРЖДАЮ
Проректор по УР
_____А.В. Бурмистров
«27» 10 2017 г.

РАБОЧАЯ ПРОГРАММА

По дисциплине Б1.В.ОД.11 «Информационная безопасность и защита информации»
Направление подготовки 09.03.02 «Информационные системы и технологии»
Профиль подготовки Информационные системы и технологии
Квалификация выпускника бакалавр
Форма обучения очная
Институт, факультет Институт технологий легкой промышленности, моды и дизайна. Факультет дизайна и программной инженерии
Кафедра-разработчик рабочей программы Информатики и прикладной математики
Курс, семестр 3,6

	Часы	Зачетные единицы
Лекции	18	0.5
Практические занятия		
Семинарские занятия		
Лабораторные занятия	36	1
Самостоятельная работа	81	2.25
Форма аттестации, экзамен	45	1.25
Всего	180	5

Казань, 2017 г.

Рабочая программа составлена с учетом требований Федерального государственного образовательного стандарта высшего образования № 219 от 12.03.2015 по направлению 09.03.02 «Информационные системы и технологии» для профиля «Информационные системы и технологии», на основании учебного плана набора обучающихся 2014, 2015 2016, 2017 года.

Разработчик программы:
к.т.н., доцент кафедры ИПМ _____ В.А.Богомолов

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и прикладной математики, протокол от 12.10 2017г. № 8

Зав. кафедрой ИПМ _____ Н.К. Нуриев

УТВЕРЖДЕНО
Протокол заседания методической комиссии факультета или института, к которому относится кафедра-разработчик РП
от 26.10 2017г. № 05-17

Председатель комиссии, профессор _____ Э.Р.Хайруллина

Начальник УМЦ _____ 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 (модуля) в структуре образовательной программы

Дисциплина «Информационная безопасность и защита информации» относится к вариативной части ОП и формирует у бакалавров по направлению подготовки Информационные системы и технологии набор знаний, умений, навыков и компетенций.

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

1) *Информатика.*
2) *Технологии информационных процессов и систем*
3) *Технологии программирования.*

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

1) *Корпоративные информационные системы*
2) *Введение в распределенные системы*
3) *Моделирование физических процессов*

Знания, полученные при изучении дисциплины «Информационная безопасность и защита информации» могут быть использованы при прохождении производственной, преддипломной практик, и выполнении выпускных квалификационных работ, могут быть использованы в научно-исследовательской, проектно-конструкторской, проектно-технологической по направлению подготовки «Информационные системы и технологии».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

1. ОПК-4 пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны
2. ПК-8 способность проводить расчет обеспечения условий безопасной жизнедеятельности

В результате освоения дисциплины обучающийся должен:

1) Знать:

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

b) способы несанкционированного доступа к компьютерной информации и способы аутентификации пользователей;

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

d) способы построения симметричных и асимметричных криптографических систем.

2) Уметь:

a) применять методы разграничения полномочий пользователей и управления доступом к ресурсам в защищенных операционных системах;

b) использовать методы и средства криптографической защиты информации;

c) применять методы и средства защиты от вредоносных программ.

3) Владеть:

a) освоить источники угроз к информационным системам;

b) изучить модели защиты информационных систем;

c) получить навыки для реализации различных моделей защиты компьютерных систем.

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

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы (в часах)				Оценочные средства для проведения промежуточной аттестации по разделам
			Лекции	Семинар	Лабораторные работы	СРС	
1	Комплексный подход к обеспечению информационной безопасности	6	2	-	4	9	тест, лабораторные работы
2	Защита от несанкционированного доступа к информации в компьютерных системах	6	4		8	18	лабораторные работы
3	Информационная безопасность и защита информации	6	4		8	18	лабораторные работы
4	Компьютерные вирусы и механизмы борьбы	6	4		8	18	тест,

	с ними						лабораторные работы
5	Защита от несанкционированного копирования информационных ресурсов	6	4		8	18	лабораторные работы
Всего			18	-	36	81	*Экзамен*

5. *Содержание лекционных занятий по темам* с указанием формируемых компетенций

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Краткое содержание	Формируемые компетенции
1	Комплексный подход к обеспечению информационной безопасности	2	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.	ОПК-4 ПК-8
2	Защита от несанкционированного доступа к информации в компьютерных системах	4	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	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.	ОПК-4 ПК-8

			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	4	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.	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.	ОПК-4 ПК-8
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	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.	ОПК-4 ПК-8

			систем. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами.		
5	Защита от несанкционированного копирования информационных ресурсов Комплексный подход к обеспечению информационной безопасности	4	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.	ОПК-4 ПК-8

6. Содержание семинарских, практических занятий (не предусмотрено учебным планом)

7. Содержание лабораторных занятий

Цель проведения лабораторных занятий – освоение лекционного материала и выработка определенных умений, связанных с использованием различных методов создания мультимедиа продуктов с использованием мультимедиа продуктов: Photoshop, Corel Draw, Flash, 3D Max, а также приобретение навыков использования интерактивной доски при чтении докладов по изучаемым темам, навыков оформления презентаций рефератов и докладов.

№ п/п	Раздел дисциплины	Часы	Наименование лабораторной работы	Формируемые компетенции
1	Комплексный подход к обеспечению информационной безопасности	4	Комплексная защита информационной системы	Комплексная защита информационной системы
2	Защита от несанкционированного доступа к информации в компьютерных системах	8	Защита от несанкционированного доступа к информации в компьютерных системах	Защита от несанкционированного доступа к информации в компьютерных системах
3 4	Информационная безопасность и защита информации Компьютерные вирусы и механизмы борьбы с ними	8	Информационная безопасность и защита информации	Информационная безопасность и защита информации
		8	Компьютерные вирусы и механизмы борьбы с ними	Компьютерные вирусы и механизмы борьбы с ними
5 1 2 3	Защита от несанкционированного копирования информационных ресурсов Комплексный подход к обеспечению информационной безопасности Защита от несанкционированного доступа к информации в компьютерных системах	8	Защита от несанкционированного копирования информационных ресурсов	Защита от несанкционированного копирования информационных ресурсов
		4	Комплексная защита	Комплексная защита

	Информационная безопасность и защита информации		информационной системы	информационной системы
		8	Защита от несанкционированного доступа к информации в компьютерных системах	Защита от несанкционированного доступа к информации в компьютерных системах
		8	Информационная безопасность и защита информации	Информационная безопасность и защита информации
4	Компьютерные вирусы и механизмы борьбы с ними	8	Компьютерные вирусы и механизмы борьбы с ними	Компьютерные вирусы и механизмы борьбы с ними

Лабораторные работы проводятся в помещении учебной лаборатории кафедры Информатики и прикладной математики.

8. Самостоятельная работа бакалавра

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Формируемые компетенции
1	Комплексный подход к обеспечению информационной безопасности	9	Изучение лекционного материала и рекомендуемой литературы; подготовка к лабораторным работам	ОПК-4 ПК-8
2	Защита от несанкционированного доступа к информации в компьютерных системах	18	Изучение лекционного материала и рекомендуемой литературы; подготовка к лабораторным работам	ОПК-4 ПК-8
3	Информационная безопасность и защита информации	18	Изучение лекционного материала и рекомендуемой литературы; подготовка к лабораторным работам; подготовка к лабораторным работам	ОПК-4 ПК-8
4	Компьютерные вирусы и механизмы борьбы с ними	18	Изучение лекционного материала и рекомендуемой литературы; подготовка к лабораторным работам	ОПК-4 ПК-8
5	Защита от несанкционированного копирования информационных ресурсов	18	Изучение лекционного материала и рекомендуемой литературы; подготовка к лабораторным работам	ОПК-4 ПК-8

9. Использование рейтинговой системы оценки знаний.

При изучении указанной дисциплины предусматривается выполнение: лабораторные работы и тесты. За эти виды работ студент может получить максимальное количество баллов – 60. В результате максимальный текущий рейтинг составит 60 баллов. На экзамене бакалавр может получить максимальное количество баллов – 40. В итоге максимальный рейтинг за

изучение дисциплины составляет 100 баллов. Экзаменационная оценка выставляется согласно данным в таблице.

Оценочные средства	***Кол-во***	***Min, баллов***	***Max, баллов***
Лабораторная работа	*9*	*27*	*45*
Контрольное тестирование	*3*	*9*	*15*
Экзамен		*24*	*40*
Итого:		***60***	***100***

10. Информационно-методическое обеспечение дисциплины

10.1. 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. Математика криптографии и теория шифрования Фороузан Б. А. Национальный Открытый Университет «ИНТУИТ» 2016 г. 511 страниц	ЭБС КнигаФонд http://www.knigafund.ru/books/178747 Доступ из любой точки интернета после регистрации с IP-адресов КНИТУ
2. Рябко Б.Я. Основы современной криптографии и стеганографии/ Фионов, А.Н..- М.: Горячия линия-Телеком,2010.- 232 с.	22 экз. в УНИЦ КНИТУ
3. Технологии защиты информации в компьютерных сетях Пролетарский А. В., Руденков Н. А., Смирнова Е. В., Суровов А. М. Национальный Открытый Университет «ИНТУИТ» 2016 г. 369 страниц	ЭБС КнигаФонд http://www.knigafund.ru/books/177241 Доступ из любой точки интернета после регистрации с IP-адресов КНИТУ
4. Администрирование ОС Linux / Гончарук С. В. - Национальный Открытый Университет «ИНТУИТ», 2016. -165 с.	ЭБС «КнигаФонд» http://www.knigafund.ru/books/176443 Доступ с любой точки интернет после регистрации по IP-адресам КНИТУ

10.2 Дополнительная литература

В качестве дополнительных источников информации, рекомендуется использовать следующею литературу:

Дополнительные источники информации	Кол-во экз.
1. Криптографические основы безопасности Лапонина О. Р. Национальный Открытый Университет «ИНТУИТ» 2016 г. 244 страницы	ЭБС КнигаФонд http://www.knigafund.ru/books/177261 Доступ из любой точки интернета после регистрации с IP-адресов КНИТУ
2. Криптографические методы защиты информации: лабораторный практикум СКФУ 2015 г. 109 страниц	ЭБС КнигаФонд http://www.knigafund.ru/books/200528 Доступ из любой точки интернета после регистрации с IP-адресов КНИТУ

1. Журнал. «Инфокоммуникационные технологии». Режим доступа: http://elibrary.ru, свободный.
2. Журнал. «Информационные системы и технологии: управление и безопасность.» Режим доступа: http://elibrary.ru, свободный.
3. Журнал. «Информация и безопасность.» Режим доступа: http://elibrary.ru, свободный.

10.3. Электронные источники информации

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

1. Электронный каталог УНИЦ КНИТУ – Режим доступа: http://ruslan.kstu.ru/
2. Научная Электронная Библиотека (НЭБ) – Режим доступа: http://elibrary.ru
3. ЭБС «Лань» – Режим доступа: http://e.lanbook.com/books/
4. ЭБС «КнигаФонд» – Режим доступа: www.knigafund.ru
5. ЭБС «БиблиоТех» – Режим доступа: https://kstu.bibliotech.ru

Согласовано:

Зав.сектором ОКУФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «КАЗАНСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ» Учебно-научный информационный центр

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

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

12. Материально-техническое обеспечение дисциплины (модуля).

В качестве материально-технического обеспечения дисциплины «Информационная безопасность и защита информации» на лекциях и лабораторных занятиях используются персональные компьютеры с выходом в Интернет и интерактивная электронная доска.

13. Образовательные технологии

Удельный вес занятий, проводимых в интерактивных формах, в учебном процессе составляет 22 % от аудиторных занятий. Занятия лекционного типа составляют 33% аудиторных занятий.

При чтении лекций используется объектно-ориентированная обучающая среда Moodle и интерактивная электронная доска. Все лабораторные занятия проводятся в компьютерных классах кафедры ИПМ с использованием электронной интерактивной доски, ПК с выходом в глобальную сеть Интернет и среды дистанционного обучения Moodle.

Основные интерактивные формы проведения учебных занятий:

• творческие задания;

• 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 РАБОЧИХ ПРОГРАММ

Рабочая программа по дисциплине «Информационная безопасность и защита информации» по направлению 09.03.02 «Информационные системы и технологии» пересмотрена на заседании кафедры Информатики и прикладной математики

№ п/п	Дата переутверждения РП (протокол заседания кафедры № _ от ____)	Наличие изменений	Наличие изменений в списке литературы	Подпись разработчика РП	Подпись заведующего кафедрой	Подпись начальника УМЦ/О Мг
1	№ 5 от 31.08.2018	нет	нет			