МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

УТВЕРЖДАЮ
Декан ФВТ
_____ Л.Р. Фионова
«_03_» _мая_ 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.35 Информационная безопасность

Направление подготовки – *09.03.03 Прикладная информатика*

Направленность (профиль подготовки) – *Прикладная информатика в экономике*

Квалификация выпускника – *бакалавр*

Форма обучения – *заочная*

Пенза, 2019

1. Цели освоения дисциплины

Целями освоения дисциплины «Информационная безопасность»является приобретение обучающимися знаний и умений по обеспечению информационной безопасности экономических информационных систем с учетом нормативно-правовой базы и основных требований информационной безопасности и применением методов и средств защиты информации от несанкционированного доступа и вредоносных программи современных информационно-коммуникационных технологий.

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина «Информационная безопасность» относится кобязательной части Блока 1 «Дисциплины (модули)» ОПОП.

Изучение дисциплины базируется на знаниях, умениях и готовностях, полученных в процессе изученияследующих дисциплин: «Математика», «Основы компьютерной обработки данных», «Основы алгоритмизации и программирования», «Программирование на языках высокого уровня»,«Вычислительные системы и сети».

Для успешного освоения дисциплины «Информационная безопасность» к «входным» знаниям, умениям и готовностям обучающихся предъявляются следующие требования: студенты должны уметь решать задачи математического анализа, знать основы построения вычислительных систем и сетей, владеть современными программными средствами разработки приложений и применять их на практике.

Компетенции, приобретенные в ходе изучения дисциплины, могут быть использованы при последующем прохождении производственной и преддипломной практик, выполнении выпускной квалификационной работы и подготовке к итоговой государственной аттестации.

3.Результаты освоения дисциплины«Информационная безопасность»

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

Коды компетенции	Наименование компетенции	Индикатор достижения компетенции	В результате освоения дисциплины обучающийся должен:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Понимает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** принципы информационной и библиографической культуры, теоретические и нормативно-правовые основы в области информационной безопасности **Уметь:** профессионально грамотно использовать на практике нормативно-правовую документацию при организации защиты информации в экономических информационных системах **Владеть:** навыками организации защиты

			информации в экономических информационных системах с учетом нормативно-правовой документации в области информационной безопасности
		ОПК-3.2. Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** методы и средства защиты информации от несанкционированного доступа и вредоносных программам в экономических информационных системах и информационно-коммуникационные технологии реализации их алгоритмов **Уметь:** анализировать риск возникновения возможных угроз информации в экономических информационных системах **Владеть:** навыками реализации основных методов и средств защиты информации при решении стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий
		ОПК-3.3. Использует методы поиска, обработки и адаптациииинформации для подготовки научно-технических документов на основе информационной и библиографической культуры, с соблюдением требований авторского права и информационной безопасности	**Знать:** основные требования информационной безопасности **Уметь:** обосновывать выбор методов и средств защиты информации от несанкционированного доступа и вредоносных программ на основе информационной и библиографической культуры и с учетом основных требований информационной безопасности

4. Структура и содержание дисциплины«Информационная безопасность»

4.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единицы, 180часов

№ п/п	Наименование разделов и тем дисциплины (модуля)	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)								Формы текущего контроля успеваемости
			Контактная работа				Самостоятельная работа				
			Всего	Лекция	Лабораторные занятия	Др. виды контакт.работы	Всего	Выполнение контрольной работы	Контроль	Подготовка к экзамену	Контрольная работа
1.	**Раздел 1. Основы информационной безопасности**	9	**2**	**2**			**48**	**48**			+
1.1.	Тема 1.1. Основные понятия в области информационной безопасности	9	1	1			12	12			+
1.2.	Тема 1.2. Правовые основы информационной безопасности	9					12	12			+
1.3.	Тема 1.3. Угрозы при передаче и обработке информации	9	1	1			12	12			+
1.4.	Тема 1.4. Методы и средства обеспечения информационной безопасности	9					12	12			+
2.	**Раздел 2. Криптографические методы защиты информации**	9	**6**	**2**	**4**		**36**	**36**			+
2.1.	Тема 2.1. Основные понятия в области криптографии	9					12	12			+
2.2.	Тема 2.2. Симметричные системы	9	3	1	2		12	12			+

	шифрования										
2.3.	Тема 2.3. Асимметричные системы шифрования	9	3	1	2		12	12			+
3.	**Раздел 3. Формирование и проверка электронной подписи**	9	**6**		**6**		**24**	**24**			+
3.1.	Тема 3.1. Хэш-код сообщения	9	2		2		12	12			+
3.2.	Тема 3.2.Электронная подпись	9	4		4		12	12			+
4.	**Раздел 4. Идентификация и аутентификация пользователей**	9					**24**	**24**			+
4.1.	Тема 4.1. Идентификация пользователей	9					12	12			+
4.2.	Тема 4.2. Аутентификация пользователей	9					12	12			+
5.	**Раздел 5. Защита информации от вредоносных программ**	9					**24,1**	**24,1**			+
5.1.	Тема 5.1. Вредоносные программы	9					12	12			+
5.2.	Тема 5.2. Способы и методы защиты информации от вредоносных программ	9					12,1	12,1			+
	Подготовка к экзамену									*36*	
	Другие виды контактной работы					*0,9*					
	Контроль								*9*		
	Общая трудоемкость, в часах		**14,9**	**4**	**10**	**0,9**	**156,1**		**9**	**36**	Промежуточная аттестация
											Форма: Экзамен; Семестр: *9*

4.2. Содержание дисциплины

4.2.1. Содержание лекционного курса

Раздел 1. Основы информационной безопасности

Тема 1.1. Основные понятия в области информационной безопасности: понятия информации, информационного ресурса, документированной информации, уровня секретности информации, конфиденциальности информации; ценность информации; категории важности информации, группы потребителей информации,качество информации и базовая система его показателей, понятие, цели и задачи информационной безопасности;

Тема 1.2.Правовые основы информационной безопасности: информация как объект права собственности, собственник и хранитель информации; право собственности на информацию, реализация права собственности на информацию, ответственность и полномочия субъектов права собственности на информацию,правовые документы о защите информации, закон Российской Федерации «Об информатизации, информационных технологиях и о защите информации».

Тема 1.3.Угрозы при передаче и обработке информации: понятие угрозы информации, факторы возникновения угроз информации, воздействие нарушителя в условиях взаимодействующих сетей, классификация угроз информации, понятие об активном и пассивном перехвате, методы криптоанализа, противодействия нападениям на защищенные сообщения;

Тема 1.4. Методы и средства обеспечения информационной безопасности: требования и принципы информационной безопасности, методы защиты информации и их классификация, средства защиты информации в экономических информационных системах,комплексные средства защиты информации.

Раздел 2. Криптографические методы защиты информации

Тема 2.1. Основные понятия в области криптографии: понятия криптологии, криптографии, криптоанализа; понятия открытого текста и шифротекста, воздействия нарушителей на криптосистемы, понятие о стойкости криптосистем, виды криптографических методов защиты информации, математические операции в криптографических системах;

Тема 2.2.Симметричные системы шифрования: принципы и схема симметричного шифрования; поточные и блочные шифры; генерация ключевой последовательности, стандарт шифрования данных AES;

Тема 2.3.Асимметричные системы шифрования: принципы и обобщенная схема асимметричного шифрования; обмен ключевой информацией, детальная схема ассиметричного шифрования, алгоритмы асимметричного шифрования RSA и Эль-Гамаля;

Раздел 3. Формирование и проверка электронной подписи

Тема 3.1. Хэш-код сообщения: понятия хэш-функции и хэш-кода сообщения, свойства хэш-кода сообщения; типовая схема вычисления хэш-кода сообщения, парадокс «Дня рождения», усложненные схемы вычисления хэш-кода сообщения, алгоритм безопасного формирования хэш-кода сообщения SHA1;

Тема 3.2.Электронная подпись: понятие электронной подписи, обобщенная и детальная схемыформирования электронной подписи, алгоритм формирования и проверки электронной подписи по Эль-Гамалю.

Раздел 4. Идентификация и аутентификация пользователей

Тема 2.1. Идентификация пользователя: понятие идентификации, методы идентификации пользователя;

Тема 2.2. Аутентификация пользователей: понятие аутентификации, методы аутентификации, многофакторная аутентификация;

Раздел5. Защита информации от вредоносных программ

Тема 5.1.Вредоносные программы: понятие вредоносной программы, классификация вредоносных программ, их функциональные возможности и наносимый ими ущерб;

Тема 5.2. Способы и методы защиты информации от вредоносных программ.

4.2.2. Перечень и содержание лабораторных занятий

№ п/п	№ разделов	Наименование лабораторных работ	Кол-вочасов
1	2	Криптографическая система защиты информации на основе стандарта AES (Rijndael)	2
2	2	Криптографическая система асимметричного шифрования RSA	2
3	3	Формирование хэш-кода сообщения на основе алгоритма SHA-1	2
4	3	Комплексная система защиты информациипо Эль-Гамалю	4

5. Образовательные технологии

В процессе изучения дисциплины применяются следующие образовательные технологии:□

- лекции с применением мультимедиа технологий

В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по собственной траектории врамках индивидуального рабочего плана, изучение данной дисциплины базируется на следующих возможностях: обеспечение внеаудиторнойработы со студентами, в том числе в электронной образовательной среде с использованием соответствующего программного оборудования,дистанционных форм обучения, возможностей интернет-ресурсов, индивидуальных консультаций и т.д.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

6.1. План самостоятельной работы студентов

№ п/п.	Раздел	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1	Основы информационной безопасности	Выполнение контрольной работы	Подготовить материалы по темеконтрольной работы	/1/, /3/, /4/	48
2	Криптографические методы защиты информации	Выполнение контрольной работы	Подготовить материалы по теме контрольной работы	1/, /3/, /4/	36
3	Формирование и проверка электронной подписи	Выполнение контрольной работы	Подготовить материалы по теме контрольной работы	1/, /3/, /4/	24
4	Идентификация и	Выполнение	Подготовить	1/, /3/, /4/	24

	аутентификация пользователей	контрольной работы	материалы по теме контрольной работы		
5	Защита информации от вредоносных программ	Выполнение контрольной работы	Подготовить материалы по теме контрольной работы	1/, /3/, /4/	24,1

6.2. Методические указания по организации самостоятельной работы студентов

Планируются следующие виды самостоятельной работы:
– работа с учебной литературой и ресурсами сети Интернет при выполнении контрольной работы;
– подготовка отчётов о выполнении лабораторных работ;
– подготовка к экзамену.

6.3. Материалы для проведения текущего ипромежуточного контроля знаний студентов

Контроль освоения компетенций

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Текущий: контрольная работа	Разделы 1 – 5	ОПК-3
2	Промежуточный: экзамен	Разделы 1 – 5	ОПК-3

Материалы для проведения текущего контроля знаний и промежуточной аттестации составляют отдельный документ – Фондоценочных средств по дисциплине «Информационная безопасность».

Демонстрационные варианты оценочных средств для каждого вида контроля смотриhttp://moodle.pnzgu.ru/course/view.php?id=57166

7. Учебно-методическое и материально-техническое обеспечение дисциплины «Информационная безопасность»

а) учебная литература:

1. Баранова, Е. К. Информационная безопасность и защита информации: Учебное пособие / Баранова Е. К., Бабаш А. В. - 3-е изд. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. (Высшее образование)

Режим доступа: https://znanium.com/catalog/product/495249

2. Бобрышева Г.В. Информационная безопасность: Методические указания к лабораторным работам / Б.А. Савельев, Г.В. Бобрышева. – Пенза: Информационно издательский центр ПГУ, 2012. – 102 с.

б) Интернет-ресурсы:

3. НОУ Интуит. Учебный курс. Криптографические методы защиты информации. [Электронный ресурс]. Режим доступаhttps://www.intuit.ru/studies/courses/13837/1234/info

4. НОУ Интуит. Учебный курс. Основы информационной безопасности.

[Электронный ресурс]. Режим доступаhttps://www.intuit.ru/studies/courses/10/10/info

в) программное обеспечение:

- среды разработки приложений (Delphi, C++, Matlab)

г) другое материально-техническое обеспечение

Для проведения лекционных занятийнеобходимааудитория, оснащённая ноутбуком, компьютерным проектором, проекционнымэкраном, шторами, сетью электропитания 220В.

Для проведения лабораторныхзанятийиспользуетсякомпьютерный класс,оборудованный локальной сетью и выходом в Internet.

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки «Прикладная информатика», утвержденного приказом Министерства образования и науки Российской Федерации от «19» сентября 2017 г. № 922.

Программу составил:
Буданов К.М. ст. преподаватель каф. «Информационно-вычислительные системы»

Программа одобрена на заседании кафедры «Информационно-вычислительные системы»

Протокол № 12 от « 02 » мая 2019 года

Зав. кафедрой ИВС Бобрышева Г.В.

Программа одобрена методической комиссией факультета вычислительной техники

Протокол № 10 от « 03 » мая 2019 года

Председатель методической комиссии факультета вычислительной техники

Т.В. Глотова

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата)	Внесенные изменения	Подпись зав. кафедрой