1920

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кубанский государственный университет»

Институт среднего профессионального образования

УТВЕРЖДАЮ
Директор ИНСПО
_____ М.Ю. Беликов
«__» _____ 20__ г.

Рабочая программа дисциплины
ОП.13 Информационная безопасность
09.02.03 Программирование в компьютерных системах

Краснодар 2016

Рабочая программа учебной дисциплины « безопасность» разработана на основе Федерального образовательного стандарта (далее – ФГОС) по специал профессионального образования (далее СПО) 09.02.03 «Про компьютерных системах», утвержденного приказом Мин 28.07.2014 № 804 (зарегистрирован в Минюсте России 33733 №

Дисциплина «Информационная безопасность»___
Форма обучения Очная_____
3 курс 6 семестр
всего 84 часов, в том числе:
лекции 40 часа.
практические занятия 20 часов.
самостоятельные занятия 20 часа.
консультации 4 часа.
форма итогового контроля контрольная ра

Составитель: преподаватель _____ Егозаров Э.
подпись

Утверждена на заседании предметно-цикловой комиссии *информатики и ИКТ»* протокол № 9 от «17» мая 2016 г.

Председатель предметно-цикловой комиссии:
_____ Н.Г. Титов
«17» мая 2016 г.

Рецензент (-ы):

Директор ООО Кахаван		
Директор ООО Альбатрос		

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

1.1. Область применения программы

Рабочая программа учебной дисциплины «Информационная безопасность» является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 09.02.03 «Программирование в компьютерных системах».

1.2. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена:

Дисциплина «Информационная безопасность» является общепрофессиональной дисциплиной обязательной части профессионального цикла, по специальности 09.02.03 Программирование в компьютерных системах в 6 семестре.

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	практический опыт (владеть)
1.	ОК-1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	сущность и понятие информационной безопасности, характеристику ее составляющих	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	
2.	ОК-2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	место информационной безопасности в системе безопасности страны	применять основные правила и документы системы сертификации Российской Федерации	
3.	ОК-3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	источники угроз информационной безопасности и меры по их предотвращению	классифицировать основные угрозы безопасности информации	
4.	ОК-4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	практический опыт (владеть)
5.	ОК-5	Использовать информационно-коммуникационные технологии в профессиональной деятельности			
6.	ОК-6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями			
8.	ОК-8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации			
9.	ОК-9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности			
12.	ПК 2.4	Реализовать методы и технологии защиты информации в базах данных	Сущность и понятие информационной безопасности, характеристику ее составляющих; Современные средства и способы обеспечения информационной безопасности.	Классифицировать основные угрозы безопасности информации.	Владеть средствами и методами защиты баз данных.
13.	ПК 3.5	Производить инспектирование компонент программного продукта на предмет соответствия стандартам кодирования	Источники угроз информационной безопасности и меры по их предотвращению.	Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;	Владеть средствами и методами защиты информации в сети.

1.3. Цели и задачи учебной дисциплины – требования к результатам освоения дисциплины:

Учебная дисциплина «Информационная безопасность» является общепрофессиональной дисциплиной обязательной части профессионального цикла ППССЗ, обуславливающей знания для профессиональной деятельности выпускника.

В результате изучения обязательной части учебного цикла обучающийся должен:

уметь:

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- применять основные правила и документы системы сертификации Российской Федерации;
- классифицировать основные угрозы безопасности информации.

знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе безопасности страны;
- источники угроз информационной безопасности и меры по их предотвращению;
- жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности.

иметь практический опыт (владеть):

- основными понятиями и моделями, стандартами безопасности;
- средствами и методами защиты информации в сети;
- средствами и методами защиты баз данных.

Максимальная учебная нагрузка обучающегося 84 часов, в том числе:

- обязательная аудиторная учебная нагрузка 60 часов;
- самостоятельная работа 20 часов;
- консультации 4 часа.

1.4. Перечень планируемых результатов обучения по дисциплине (перечень формируемых компетенций)

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	практический опыт (владеть)
1.	ОК-1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.			
2.	ОК-2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.			
3.	ОК-3	Принимать решения в			

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	практический опыт (владеть)
		стандартных и нестандартных ситуациях и нести за них ответственность			
4.	ОК-4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.			
5.	ОК-5	Использовать информационно-коммуникационные технологии в профессиональной деятельности			
6.	ОК-6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями			
8.	ОК-8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации			
9.	ОК-9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности			
12.	ПК 2.4	Реализовать методы и технологии защиты информации в базах данных	Сущность и понятие информационной безопасности, характеристику ее составляющих; Современные средства и способы обеспечения информационной безопасности.	Классифицировать основные угрозы безопасности информации.	Владеть средствами и методами защиты баз данных.
13.	ПК 3.5	Производить инспектирование	Источники угроз информационной	Классифицировать защищаемую	Владеть средствами и методами защиты

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	практический опыт (владеть)
		компонент программного продукта на предмет соответствия стандартам кодирования	безопасности и меры по их предотвращению.	информацию по видам тайны и степеням конфиденциальности;	информации в сети.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	84
Обязательная аудиторная учебная нагрузка (всего)	60
в том числе:	
занятия лекционного типа	40
практические занятия	20
Самостоятельная работа обучающегося (всего)	20
Консультации	4
Промежуточная аттестация в форме зачета/экзамена/дифзачета	*Зачет*

2.2. Структура дисциплины:

Наименование разделов и тем	**Количество аудиторных часов**			**Самостоятельная работа обучающегося (час)**	**Консультации**
	Всего	**Теоретическое обучение**	**Практические и лабораторные занятия**		
Раздел 1. Основы информационной безопасности	21	10	3	8	-
Раздел 2. Криптографические методы информационной безопасности	17	10	3	4	-
Раздел 3. Методы и средства защиты информации	18	10	4	4	-
Раздел 4. Аппаратные и программные средства защиты компьютерной информации	24	10	10	4	-
Всего по дисциплине	**80**	**40**	**20**	**20**	**4**

2.3. Тематический план и содержание учебной дисциплины «Информационная безопасность»

Наименование разделов и тем	**Содержание учебного материала, практические работы, самостоятельная работа обучающихся, курсовая работа (если предусмотрена)**		**Объем часов**	**Уровень освоения**
1	**2**		**3**	**4**
Раздел 1. Основы информационной безопасности			**21**	
	Содержание учебного материала			
	Лекции			1
	1	Вводное занятие. Основные понятия защиты информации	2	2
	2	Общие проблемы защиты информации. Безопасность в информационной среде. Классификация средств защиты	2	2
	3	Угрозы информационной безопасности и каналы утечки информации	2	1
	4	Инженерно-технические средства защиты информации. Программно-аппаратные средства защиты	4	2
	Практические (лабораторные) занятия		3	
	1	Шифрование текста по ключу методами замены	1	
	2	Шифрование текста по ключу методами перестановки	1	

	3	Методы шифрования текста при помощи аналитических преобразований	1	
	Самостоятельная работа обучающихся 1. Преднамеренные умышленные угрозы. Традиционный шпионаж и диверсии 2. Стандарт ISO/IES 15408 «Критерии оценки безопасности информационных технологий» 3. Обзор зарубежного законодательства в области информационной безопасности		8	
Раздел 2. Криптографические методы информационной безопасности			**17**	
	Содержание учебного материала			
	Лекции			
	1	История криптографической деятельности. Основные понятия, определения, композиции и синтез шифров. Простейшие шифры с симметричными ключами: замены	2	1
	2	Простейшие шифры с симметричными ключами: перестановки. Простейшие шифры с симметричными ключами: гаммирование	2	2
	3	Шифрование с симметричными ключами при помощи аналитических преобразований. Смешанные методы шифрования. Криптографические системы DES и ГОСТ 28147-89	2	2
	4	Асимметричные шифры. Системы с открытыми ключами. Системы с открытыми ключами. Электронно-цифровая подпись	2	2
	5	Криптографические протоколы: аутентификации, обмена ключами. Специфические протоколы. Оценка криптостойкости шифров. Элементы криптоанализа	2	2
	Практические (лабораторные) занятия		3	
	1	Шифрование текста по ключу аддитивными методами (гаммированием)	1	
	2	Шифры с открытым ключом. Алгоритм RSA	1	
	3	Методы парольной защиты. Разработка программной парольной защиты	1	
	Самостоятельная работа обучающихся 1. Обзор российского законодательства в области информационной безопасности 2. Требования к блочному алгоритму шифрования 3. Сеть Фейштеля		4	
Раздел 3. Методы и средства защиты информации			**18**	
	Содержание учебного материала			
	Лекции			
	1	Стеганография. Становление как науки. Компьютерная стеганография и её применение	2	1
	2	Туннелирование. Управление. Обеспечение отказоустойчивости и обслуживаемости	2	3
	3	Методы идентификации и аутентификации пользователей на основе паролей	2	2
	4	Аутентификация пользователя по биометрическим характеристикам	2	3
	5	Парольная защита. Способы атаки на пароль. Обеспечение безопасности пароля	2	2
	Практические (лабораторные) занятия		4	
	1	Количественная оценка стойкости парольной защиты. Генератор паролей, обладающий требуемой стойкостью к взлому	1	
	2	Количественная оценка стойкости парольной защиты. Генератор паролей, обладающий требованиями к парольным генераторам	1	
	3	Пакеты антивирусных программ. Профилактика заражения вирусами компьютерных систем	2	
	Самостоятельная работа обучающихся 1. Обзор алгоритмов формирования хеш-функций 2. Поточные шифры и генераторы псевдослучайных чисел 3. Сервисы безопасности: экранирование, туннелирование		4	
Раздел 4. Аппаратные и программные средства защиты компьютерной информации			**24**	
	Содержание учебного материала			
	Лекции			
	1	Компьютерные вирусы и средства защиты от них. Характер проявления компьютерных вирусов. Компьютерная преступность. Разновидности	2	3

		компьютерного пиратства		
	2	Угрозы информационной безопасности при подключении к Интернет. Методы взлома интрасетей. Обзор технических и программных средств обеспечения безопасности компьютерных сетей	2	3
	3	Средства защиты сети: межсетевые экраны, виртуальные частные сети, системы обнаружения вторжений. Средства защиты информации от несанкционированного доступа	2	2
	4	Защита от несанкционированного доступа в операционной системе Windows. Защита документов в Microsoft Office. Защита баз данных. Организационно-правовое обеспечение информационной безопасности	2	3
	5	Актуальные проблемы уголовно-правовой борьбы с посягательствами на компьютерную информацию.	2	2
	Практические (лабораторные) занятия		10	
	1	Криптографическая защита электронной почты. Программный пакет шифрования PGP	2	
	2	Защита от закладок при разработке программ. Исследование и анализ служебных программ Windows для повышения эффективности работы компьютера	2	
	3	Защита баз данных на примере MS Access №1	2	
	4	Защита баз данных на примере MS Access №2	2	
	5	Подготовка отчетов. Защита выполненных работ	2	
	Самостоятельная работа обучающихся 1. Использование карт идентификации/аутентификации 2. Формы проявления компьютерной преступности: хищение машинного времени, саботаж, компьютерное 3. Пути и проблемы практической реализации концепции комплексной защиты информации		4	
	Всего:		**80**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);

2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)

3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

2.4. Содержание разделов дисциплины

2.4.1. Занятия лекционного типа

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
6 семестр			
1	Основы информационной безопасности	Вводное занятие. Основные понятия защиты информации. Общие проблемы защиты информации. Безопасность в информационной среде. Классификация средств защиты. Угрозы информационной безопасности и каналы утечки информации. Инженерно-технические средства защиты информации. Программно-аппаратные средства защиты.	ПР

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
2	Криптографические методы информационной безопасности	История криптографической деятельности. Основные понятия, определения, композиции и синтез шифров. Простейшие шифры с симметричными ключами: замены. Простейшие шифры с симметричными ключами: перестановки. Простейшие шифры с симметричными ключами: гаммирование. Шифрование с симметричными ключами при помощи аналитических преобразований. Смешанные методы шифрования. Криптографические системы DES и ГОСТ 28147-89. Асимметричные шифры. Системы с открытыми ключами. Системы с открытыми ключами. Электронно-цифровая подпись. Криптографические протоколы: аутентификации, обмена ключами. Специфические протоколы. Оценка криптостойкости шифров. Элементы криптоанализа.	ПР
3	Методы и средства защиты информации	Стеганография. Становление как науки. Компьютерная стеганография и её применение. Туннелирование. Управление. Обеспечение отказоустойчивости и обслуживаемости. Методы идентификации и аутентификации пользователей на основе паролей Аутентификация пользователя по биометрическим характеристикам. Парольная защита. Способы атаки на пароль. Обеспечение безопасности пароля.	ПР
4	Аппаратные и программные средства защиты компьютерной информации	Компьютерные вирусы и средства защиты от них. Характер проявления компьютерных вирусов. Компьютерная преступность. Разновидности компьютерного пиратства. Угрозы информационной безопасности при подключении к Интернет. Методы взлома интрасетей. Обзор технических и программных средств обеспечения безопасности компьютерных сетей. Средства защиты сети: межсетевые экраны, виртуальные частные сети, системы обнаружения вторжений. Средства защиты информации от несанкционированного доступа. Защита от несанкционированного доступа в операционной системе Windows. Защита документов в Microsoft Office. Защита баз данных. Организационно-правовое обеспечение информационной безопасности. Актуальные проблемы уголовно-правовой борьбы с посягательствами на компьютерную информацию.	ПР
Примечание: Т – тестирование, Р – написание реферата, У – устный опрос, КР – контрольная работа			

2.4.2. Занятия семинарского типа

Не предусмотрено

2.4.3. Практические занятия (Лабораторные занятия)

№	Наименование раздела	Наименование практических (лабораторных) работ	Форма текущего контроля
6 семестр			
1	2	3	4
1	Основы информационной безопасности	Шифрование текста по ключу методами замены	ПР
		Шифрование текста по ключу методами перестановки	
		Методы шифрования текста при помощи аналитических преобразований	
2	Криптографические методы	Шифрование текста по ключу аддитивными методами (гаммированием)	ПР

	информационной безопасности	Шифры с открытым ключом. Алгоритм RSA	
		Методы парольной защиты. Разработка программной парольной защиты	
3	Методы и средства защиты информации	Количественная оценка стойкости парольной защиты. Генератор паролей, обладающий требуемой стойкостью к взлому	ПР
		Количественная оценка стойкости парольной защиты. Генератор паролей, обладающий требованиями к парольным генераторам	
		Пакеты антивирусных программ. Профилактика заражения вирусами компьютерных систем	
4	Аппаратные и программные средства защиты компьютерной информации	Криптографическая защита электронной почты. Программный пакет шифрования PGP	ПР
		Защита от закладок при разработке программ. Исследование и анализ служебных программ Windows для повышения эффективности работы компьютера	
		Защита баз данных на примере MS Access	
		Подготовка отчетов. Защита выполненных работ	

Примечание: ПР- практическая работа, ЛР- лабораторная работа; Т – тестирование, Р – написание реферата, У – устный опрос, КР – контрольная работа

2.4.4. Содержание самостоятельной работы

№	Наименование раздела	Наименование самостоятельных работ
1	2	3
1	Основы информационной безопасности	Преднамеренные умышленные угрозы. Традиционный шпионаж и диверсии Стандарт ISO/IES 15408 «Критерии оценки безопасности информационных технологий» Обзор зарубежного законодательства в области информационной безопасности
2	Криптографические методы информационной безопасности	Обзор российского законодательства в области информационной безопасности Требования к блочному алгоритму шифрования Сеть Фейштеля
3	Методы и средства защиты информации	Обзор алгоритмов формирования хеш-функций Поточные шифры и генераторы псевдослучайных чиселСервисы безопасности: экранирование, туннелирование
4	Аппаратные и программные средства защиты компьютерной информации	Использование карт идентификации/аутентификации Формы проявления компьютерной преступности: хищение машинного времени, саботаж. Пути и проблемы практической реализации концепции комплексной защиты информации

2.4.5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

На самостоятельную работу обучающихся отводится 24 часов учебного времени.

Самостоятельная работа учащихся в процессе освоения дисциплины включает:

- изучение основной и дополнительной литературы по предмету;
- изучение (конспектирование) вопросов, вызывающих затруднения при их изучении;
- работу с электронными учебными ресурсами;
- изучение материалов периодической печати, интернет ресурсов;
- подготовку к тестированию;
- подготовку к практическим и лабораторным занятиям,
- выполнение домашних заданий.

№	Наименование раздела, темы, вида СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1.	Основы информационной безопасности	Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет» ; авт.-сост. М.А. Лапина, Д.М. Марков и др. - Ставрополь : СКФУ, 2016. - 242 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458012
2.	Криптографические методы информационной безопасности	Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557
3.	Методы и средства защиты информации	Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557
4.	Аппаратные и программные средства защиты компьютерной информации	Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

3. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

3.1.Образовательные технологии при проведении лекций

№	Тема	Виды применяемых образовательных технологий	Кол-во час
1	2	3	4
1	Инженерно-технические средства защиты информации. Программно-аппаратные средства защиты	Презентация; Проблемное изложение.	2
2	История криптографической деятельности. Основные понятия, определения, композиции и синтез шифров. Простейшие шифры с симметричными ключами: замены	Презентация; Проблемное изложение.	2
3	Аутентификация пользователя по биометрическим характеристикам	Презентация; Проблемное изложение.	2
4	Угрозы информационной безопасности при подключении к Интернет. Методы взлома интрасетей. Обзор технических и программных средств обеспечения безопасности компьютерных сетей	Презентация; Проблемное изложение.	2
5	Защита от несанкционированного доступа в операционной системе Windows. Защита документов в Microsoft Office. Защита баз данных. Организационно-правовое обеспечение информационной безопасности	Презентация; Проблемное изложение.	2
	Итого по курсу		40
	в том числе интерактивное обучение*		10

3.2.Образовательные технологии при проведении практических занятий (лабораторных работ)

№	Тема занятия	Виды применяемых образовательных технологий	Кол. час
1.	Шифрование текста по ключу методами замены	Презентация; Проблемное изложение.	2
2.	Шифрование текста по ключу методами перестановки	Презентация; Проблемное изложение.	2
3.	Методы парольной защиты. Разработка программной парольной защиты	Презентация; Проблемное изложение.	2
4.	Количественная оценка стойкости парольной защиты. Генератор паролей, обладающий требованиями к парольным генераторам	Презентация; Проблемное изложение.	2
5.	Криптографическая защита электронной почты. Программный пакет шифрования PGP	Презентация; Проблемное изложение.	2
6.	Защита от закладок при разработке программ. Исследование и анализ служебных программ Windows для повышения эффективности работы компьютера	Презентация; Проблемное изложение.	2
7.	Защита баз данных на примере MS Access	Презентация; Проблемное изложение.	2
	Итого по курсу		20
	в том числе интерактивное обучение*		14

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

4.1. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Лаборатория информационных технологий в профессиональной деятельности, ул. Мира, 29 ауд. 5

Оснащенность:

- специализированная мебель и системы хранения (доска классная, стол и стул учителя, столы и стулья ученические, шкафы для хранения учебных пособий, системы хранения таблиц и плакатов);
- технические средства обучения (рабочее место учителя: компьютер учителя, видеопроектор, экран, лицензионное ПО);
- демонстрационные учебно-наглядные пособия (комплект стендов).

4.2. Перечень необходимого программного обеспечения

- Операционная система Microsoft Windows 10 (контракт №104-АЭФ/2016 от 20.07.2016, корпоративная лицензия);
- Пакет программ Microsoft Office Professional Plus (контракт №104-АЭФ/2016 от 20.07.2016, корпоративная лицензия);
- Антивирусная защита физических рабочих станций и серверов: Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 1500-2499 Node 1 year Educational Renewal License (контракт №99-АЭФ/2016 от 20.07.2016, корпоративная лицензия);
- Lazarus – открытая среда разработки программного обеспечения на языке Object Pascal (свободное программное обеспечение, не ограничено, бессрочно);
- GIMP – свободно распространяемый растровый графический редактор, используемый для создания и обработки растровой графики License (свободное программное обеспечение, не ограничено, бессрочно);
- 7-zip GNULesser General Public License (свободное программное обеспечение, не ограничено, бессрочно);
- Интернет браузер Google Chrome (бесплатное программное обеспечение, не ограничено, бессрочно);
- K-Lite Codec Pack — универсальный набор кодеков (кодировщиков-декодировщиков) и утилит для просмотра и обработки аудио- и видеофайлов (бесплатное программное обеспечение, не ограничено, бессрочно);
- WinDjView – программа для просмотра файлов в формате DJV и DjVu (свободное программное обеспечение, не ограничено, бессрочно);

5. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

5.1. Основная литература

1. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет» ; авт.-сост. М.А. Лапина, Д.М. Марков и др. - Ставрополь : СКФУ, 2016. - 242 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458012

5.2. Дополнительная литература

1. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

5.3. Периодические издания

1. Журнал Открытые системы. СУБД
2. Журнал Программирование.
3. Электронная библиотека "Издательского дома "Гребенников" (www.grebennikon.ru).
4. Базы данных компании «Ист Вью» (http://dlib.eastview.com).

5.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Министерство образования и науки Российской Федерации (http://минобрнауки.рф/);
2. Федеральный портал "Российское образование" (http://www.edu.ru/);
3. Информационная система "Единое окно доступа к образовательным ресурсам" (http://window.edu.ru/);
4. Единая коллекция цифровых образовательных ресурсов (http://school-collection.edu.ru/);
5. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
6. Образовательный портал "Учеба" (http://www.ucheba.com/);
7. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" (https://pushkininstitute.ru/);
8. Научная электронная библиотека (НЭБ) (http://www.elibrary.ru);
9. Национальная электронная библиотека (http://нэб.рф/);

10. КиберЛенинка (http://cyberleninka.ru/).
11. Справочно-информационный портал "Русский язык" (http://gramota.ru/);
12. Служба тематических толковых словарей (http://www.glossary.ru/);
13. Словари и энциклопедии (http://dic.academic.ru/);
14. Консультант Плюс - справочная правовая система (доступ по локальной сети)

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учащиеся для полноценного освоения учебного курса «Информационная безопасность» должны составлять конспекты как при прослушивании его теоретической (лекционной) части, так и при подготовке к практическим занятиям. Желательно, чтобы конспекты лекций и семинаров записывались в логической последовательности изучения курса и содержались в одной тетради. Это обеспечит более полную подготовку как к текущим учебным занятиям, так и сессионному контролю знаний.

Самостоятельная работа учащихся является важнейшей формой учебно-познавательного процесса. Цель заданий для самостоятельной работы – закрепить и расширить знания, умения, навыки, приобретенные в результате изучения дисциплины; овладеть умением использовать полученные знания в практической работе; получить первичные навыки профессиональной деятельности.

Началом организации любой самостоятельной работы должно быть привитие навыков и умений грамотной работы с учебной и научной литературой. Этот процесс, в первую очередь, связан с нахождением необходимой для успешного овладения учебным материалом литературой. Учащийся должен изучить список нормативно-правовых актов и экономической литературы, рекомендуемый по учебной дисциплине; уметь пользоваться фондами библиотек и справочно-библиографическими изданиями.

Задания для самостоятельной работы выполняются в письменном виде во внеаудиторное время. Работа должна носить творческий характер, при ее оценке преподаватель в первую очередь оценивает обоснованность и оригинальность выводов. В письменной работе по теме задания учащийся должен полно и всесторонне рассмотреть все аспекты темы, четко сформулировать и аргументировать свою позицию по исследуемым вопросам. Выбор конкретного задания для самостоятельной работы проводит преподаватель, ведущий практические занятия в соответствии с перечнем, указанным в планах практических занятий.

7. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ УСПЕВАЕМОСТИ

7.1. Паспорт фонда оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Основы информационной безопасности	ПК 2.4; ПК 3.5; ОК 1 – ОК 6; ОК 8 – ОК 9.	Практическая работа
2.	Криптографические методы информационной безопасности	ПК 2.4; ОК 1 – ОК 6; ОК 8 – ОК 9.	Практическая работа
3.	Методы и средства защиты информации	ПК 2.4; ПК 3.5 ОК 1 – ОК 6; ОК 8 – ОК 9.	Практическая работа
4.	Аппаратные и программные средства защиты компьютерной информации	ПК 3.5; ПК 2.4; ОК 1 – ОК 6; ОК 8 – ОК 9.	Практическая работа

7.2. Критерии оценки знаний

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических работ, тестирования, собеседования по результатам выполнения лабораторных работ, а также решения задач, составления рабочих таблиц и подготовки сообщений к уроку. Знания студентов на практических занятиях оцениваются отметками «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Оценка «отлично» выставляется, когда студент показывает глубокое всестороннее знание раздела дисциплины, обязательной и дополнительной литературы, аргументировано и логически стройно излагает материал, может применять знания для анализа конкретных ситуаций.

Оценка «хорошо» ставится при твердых знаниях раздела дисциплины, обязательной литературы, знакомстве с дополнительной литературой, аргументированном изложении материала, умении применить знания для анализа конкретных ситуаций.

Оценка «удовлетворительно» ставится, когда студент в основном знает раздел дисциплины, может практически применить свои знания.

Оценка «неудовлетворительно» ставится, когда студент не освоил основного содержания предмета и слабо знает изучаемый раздел дисциплины.

7.3. Оценочные средств для проведения текущей аттестации

Форма аттестации	Знания	Умения	Практический опыт (владение)	Личные качества обучающегося	Примеры оценочных средств
Тестирование	Контроль знаний по определенным проблемам	Оценка умения различать конкретные понятия	Оценка навыков логического анализа понятий	Оценка способности оперативно и качественно отвечать на поставленные вопросы	Вопросы прилагаются
Устный (письменный) опрос по темам	Контроль знаний по определенным проблемам	Оценка умения различать конкретные понятия	Оценка навыков работы с литературными источниками	Оценка способности оперативно и качественно отвечать на поставленные вопросы	Контрольные вопросы по темам прилагаются
Практические (лабораторн	криптографию, стеганографи	составлять криптосистемы; манипулироват	Основными понятиями и моделями,	Оценка способности оперативно и качественно решать	Темы работ прилагаются

ые) работы	ю, аутентификацию, невозможность отказа от авторства; политику безопасности в мировых законах и законах РФ; криптографические методы и алгоритм; алгоритмы криптоанализа; алгоритмы идентификации пользователя на биометрических принципах; средства защиты сетей и нормативные требования к системам защиты информации;	ь с данными; выбирать наиболее подходящий из методов защиты информации	стандартами безопасности; криптографическими методами; средствами и методами защиты информации в сети;	поставленные на практических и лабораторных работах задачи и аргументировать результаты	

Примерные тестовые задания:

1. Разработка программ обеспечения информационной безопасности РФ и определение порядка их финансирования относится к:

- правовым методам защиты информации
- организационно-техническим методам защиты информации
- организационно-распорядительным методам защиты информации
- нормативно-правовым методам защиты информации
- экономическим методам защиты информации

2. К какому виду конфиденциальной информации относится научно-техническая, технологическая, производственная, финансово-экономическая и иная деловая информация, в том числе информация о секретах производства?

- коммерческая тайна
- персональные данные
- государственная служебная тайна
- процессуальная тайна

3. Какой канал утечки информации основан на использовании электромагнитной энергии видимого и инфракрасного диапазона?

- визуально-оптический канал
- электромагнитный канал
- виброакустический канал

– материально-вещественный канал

Примерные вопросы для устного опроса (контрольных работ):

1. Классификация угроз безопасности ИС.
2. Перехват паролей, вредоносные программы, незаконное использование привелегий, маскарад.
3. Sniffing.

Примерные вопросы для контроля самостоятельной работы:

1. Угрозы и уязвимости в беспроводных сетях.
2. Подходы обеспечения информационной безопасности.
3. Меры обеспечения информационной безопасности.

7.4. Оценочные средств для проведения промежуточной аттестации

Промежуточная аттестация

Форма аттестации	Знания	Умения	Практический опыт (владеть)	Личные качества обучающегося	Примеры оценочных средств
Зачет	криптографию, стеганографию, аутентификацию, невозможность отказа от авторства; политику безопасности в мировых законах и законах РФ; криптографические методы и алгоритм; алгоритмы криптоанализа; алгоритмы идентификации пользователя на биометрических принципах; средства защиты сетей и нормативные требования к системам защиты информации;	составлять криптосистемы; манипулировать с данными; выбирать наиболее подходящий из методов защиты информации	Основными понятиями и моделями, стандартами безопасности; криптографическими методами; средствами и методами защиты информации в сети;	Оценка способности грамотно и четко излагать материал в области профессиональной деятельности и аргументировать результаты	Вопросы: прилагаются

7.4.1. Примерные вопросы для проведения промежуточной аттестации (зачет)

1. Основные понятия информационной безопасности.
2. Основные понятия защиты информации.
3. Объект информатизации, собственник информации, владелец информации, информационный актив, политика безопасности.
4. Уровни информационной безопасности ИС, для информационных ресурсов. Угрозы.
5. Классификация угроз безопасности ИС.
6. Перехват паролей, вредоносные программы, незаконное использование привелегий, маскарад.
7. Sniffing.
8. Hijacking.
9. Session Hijacking.
10. Атаки модификации.
11. Атаки отказа в обслуживании.
12. Комбинированные атаки.
13. Фарминг.
14. Ботнет.
15. Угрозы и уязвимости в беспроводных сетях.
16. Подходы обеспечения информационной безопасности.
17. Меры обеспечения информационной безопасности.
18. Политика информационной безопасности.
19. Структура политики безопасности организации.
20. Международные стандарты информационной безопасности.
21. Российские стандарты информационной безопасности.
22. Угрозы безопасности операционных систем.
23. Административные меры защиты в операционных системах.
24. Политика безопасности операционной системы.
25. Криптографическая защита информации.
26. Административные действия пользователя.
27. Строгая аутентификация.
28. Аутентификация на основе USB или смарт-карт.
29. Безопасность беспроводных сетей.
30. Межсетевой экран и его функциональные возможности.
31. Межсетевой экран и дополнительные функции.
32. VPN сеть.
33. VPN для создания защищенной сети.
34. VPN с удаленным доступом.
35. VPN внутрикорпоративная.
36. VPN межкорпоративная.
37. Задачи управления информационной безопаностью в корпоративной информационной системе.
38. Проблемы безопасности облачных сервисов.
39. Средства защиты в виртуальных средах.

40. Смарт-карта.

7.4.2. Примерные экзаменационные задачи на экзамен/диф зачет

Не предусмотрено

8. ОБУЧЕНИЕ СТУДЕНТОВ-ИНВАЛИДОВ И СТУДЕНТОВ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Порядок обучения инвалидов и студентов с ограниченными возможностями определен «Положением КубГУ об обучении студентов-инвалидов и студентов с ограниченными возможностями здоровья».

Для лиц с ограниченными возможностями здоровья предусмотрены образовательные технологии, учитывающие особенности и состояние здоровья таких лиц.

9. ДОПОЛНИТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

не предусмотрено

Рецензия

на рабочую программу учебной дисциплины ОП.13 Информационная безопасность для студентов, обучающихся по направлению 09.02.03 «Программирование в компьютерных системах».

Рабочая программа учебной дисциплины ОП.13 Информационная безопасность предназначена для реализации государственных требований к уровню подготовки выпускников по специальности среднего профессионального образования, 09.02.03 «Программирование в компьютерных системах». Разработчик программы – преподаватель «КубГУ», факультета ИНСПО, Егозаров Эдуард Сергеевич.

Рабочая программа дисциплины ОП.13 Информационная безопасность содержит следующие элементы: титульный лист, паспорт (указана область применения программы, место дисциплины в структуре основной образовательной программы, цели и задачи, объем учебной дисциплины и виды учебной работы); тематический план и содержание учебной дисциплины, условия реализации программы (требования к минимальному материально-техническому обеспечению, перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы); контроль и оценка результатов освоения учебной дисциплины.

Рабочая программа рассчитана на 84 часа, из которых 28 часов отводится на практические и лабораторные занятия, а лекционных занятий 32 часа. Самостоятельная работа составляет 20 часов учебного времени. И 4 часа отводится на консультации.

Рабочая программа может быть рекомендована для использования в образовательном процессе ФГБОУ ВО «Кубанский государственный университет».

Рецензент:

Директор ООО Альбатрос	Краснодарский край г. Краснодар Общество с ограниченной ответственностью «Альбатрос» Российская Федерация	[illegible]

Рецензия
на рабочую программу учебной дисциплины
ОП.13 Информационная безопасность
для специальности 09.02.03 Программирование в компьютерных системах

Рабочая программа учебной дисциплины ОП.13 Информационная безопасность разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) 09.02.03 «Программирование в компьютерных системах», утвержденного приказом Минобрнауки РФ от 28.07.2014 г № 804 (зарегистрирован в Минюсте России 21.08.2014 г. № 33733).

Обучение проводится на базе основного общего образования и нацелено на получение квалификации техник-программист. Рабочая программа составлена для очной формы обучения.

Паспорт программы обоснованно и полно отражает содержание дисциплины, ее роль и место в подготовке специалиста среднего звена, раскрывает цели и задачи учебной дисциплины. Определены требования к умениям и знаниям студентов. Тематический план и содержание учебной дисциплины раскрывает последовательность прохождения тем, соответствует тематическому плану и распределению часов. В программе определены форма проведения, цели, задачи учебной дисциплины, представлены обязательные формы отчетности. В программе реализованы дидактические принципы обучения: целостность, структурность; отражена взаимосвязь между элементами структуры, учтены межпредметные связи. Изучение данной дисциплины способствует эффективной и качественной подготовке студентов.

Программа учебной дисциплины направлена на формирование у студента приобретению практического опыта и соответствует требованиям к результатам освоения предмета.

Перечень рекомендуемой основной и дополнительной литературы включает общедоступные источники, изданные в последнее время (не позднее 5 лет). Перечисленные Интернет-ресурсы актуальны и достоверны.

Разработанная программа учебной дисциплины может быть рекомендована для использования в учебном процессе при подготовке по специальности 09.02.03 Программирование в компьютерных системах.

Директор ООО Караван	Удмуртская Республика г.Ижевск Октябрьский район Общество с ограниченной ответственностью Образовательное подразделение «КАРАВАН» г.Краснодар ИНН 1831107435 ОГРН 1051800639043	Машков М.С