1920

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Кубанский государственный университет» в г. Геленджике

УТВЕРЖДАЮ
Проректор по работе с филиалами
_____ А.А. Евдокимов
«1» августа 2017 г.

Рабочая программа дисциплины
ОП.11 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

специальность 09.02.03 Программирование в компьютерных системах

2017

Рабочая программа учебной дисциплины ОП.11 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 №804 (зарегистрирован в Минюсте России 21.08.2014 № 33733)

Дисциплина **ОП.11 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**
Форма обучения очная
Учебный год 2017-2018

4 курс	7 семестр
лекции	40 час.
практические занятия	20 час.
самостоятельные занятия	30 час.
форма итогового контроля	экзамен

Составитель: преподаватель _____ Л.Л. Левин канд.техн.наук
подпись

Утверждена на заседании предметной (цикловой) комиссии профессиональных дисциплин программирования и компьютерных систем
Протокол № 1 от 31 августа 2017 г.

Председатель предметной (цикловой) комиссии профессиональных дисциплин программирования в компьютерных системах _____ Л.А. Благова

Рецензенты:

Директор ООО «ТКМ» г. Геленджик	_____ *подпись, печать*	Л.В. Приходько
Заместитель директора директора ООО «Компания «ИНКОМТЕХ»	_____ *подпись, печать*	О.В. Брызгалов

ЛИСТ

согласования рабочей учебной программы по дисциплине

ОП.11 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Специальность среднего профессионального образования:
09.02.03 Программирование в компьютерных системах

СОГЛАСОВАНО:

Зам. директора по УР филиала _____ Т. А. Резуненко
«31» августа 2017г.

Заведующая сектором библиотеки _____ Л. Г. Соколова
«31» августа 2017г.

Инженер-электроник (программно-информационное обеспечение образовательной программы) _____ А. В. Сметанин
«31» августа 2017г.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 5
1.1 Область применения программы 5
1.2. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена: 5
1.3. Цели и задачи учебной дисциплины – требования к результатам освоения дисциплины: 5
1.4. Перечень планируемых результатов обучения по дисциплине (перечень формируемых компетенций) 6
2.СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ 9
2.1. Объем учебной дисциплины и виды учебной работы 9
2.2. Структура дисциплины: 9
2.3. Тематический план и содержание учебной дисциплины 10
2.4. Содержание разделов дисциплины 13
2.4.1. Занятия лекционного типа 13
2.4.2. Занятия семинарского типа 13
2.4.3. Практические занятия 13
2.4.4. Содержание самостоятельной работы (Примерная тематика рефератов) 14
2.4.5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине 15
3. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ 17
3.1.Образовательные технологии при проведении лекций 17
3.2.Образовательные технологии при проведении практических занятий 17
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ 18
4.1. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине 18
4.2. Перечень необходимого программного обеспечения 19
5. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ 20
5.1. Основная литература 20
5.2. Дополнительная литература 20
5.3. Периодические издания 21
5.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины 22
6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ 23
7. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ УСПЕВАЕМОСТИ 24
7.1. Паспорт фонда оценочных средств 24
7.2. Критерии оценки знаний 24
7.3. Оценочные средств для проведения для текущей аттестации 25
7.4. Оценочные средств для проведения промежуточной аттестации 27
7.4.1. Примерные вопросы для проведения промежуточной аттестации 27
7.4.2. Примерные задачи для проведения промежуточной аттестации 28
8. ДОПОЛНИТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 29

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.11 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Область применения программы

Рабочая программа учебной дисциплины **ОП.11 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 ОП.11 Информационная безопасность входит в **вариативную часть** ППССЗ.

Для освоения дисциплины студенты используют знания, умения и навыки, сформированные при изучении предметов: Основы программирования, Физика, Прикладное программирование, Операционные системы и др.

Изучение дисциплины «**ОП.11 Информационная безопасность**» предваряет Производственную и Преддипломную практики.

1.3. Цели и задачи учебной дисциплины ОП.11 Информационная безопасность – требования к результатам освоения

Целью освоения учебной дисциплины «Информационная безопасность» является приобретение теоретических и практических умений и навыков применения современных информационных технологий для использования в профессиональной деятельности по защите информации.

Задачи:

- формирование у обучающихся общего представления о современных концепциях информационной безопасности;
- знакомство с различными методами защиты информации от несанкционированного доступа;
- изучение криптографических средств, как основного инструмента обеспечения сохранности компьютерной информации;
- приобретение практических навыков работы с современными аппаратными и программными средствами защиты информации.

В результате изучения профессионального модуля 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 национальной 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;

Максимальная учебная нагрузка обучающегося 90 часов, в том числе:
- обязательная аудиторная учебная нагрузка обучающегося 60 часа;
- самостоятельная работа обучающегося 30 часа.

1.4. Перечень планируемых результатов обучения по дисциплине ОП.11 Информационная безопасность

Учащийся должен обладать **общими** и **профессиональными компетенциями**, включающими в себя способности:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК 1.1. Выполнять разработку спецификаций отдельных компонент.

ПК 1.2. Осуществлять разработку кода программного продукта на основе готовых спецификаций на уровне модуля.

ПК 2.3. Решать вопросы администрирования базы данных.

ПК 2.4. Реализовывать методы и технологии защиты информации в базах данных.
ПК 3.1. Анализировать проектную и техническую документацию на уровне взаимодействия компонент программного обеспечения.
ПК 3.4. Осуществлять разработку тестовых наборов и тестовых сценариев.
ПК 3.6. Разрабатывать технологическую документацию.

Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
		знать	уметь	иметь практический опыт
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	сущность и социальную значимость будущей профессии.	проявлять к будущей профессии устойчивый интерес	-повышение успеваемости по МДК, положительный отзыв руководителя практики. -систематического посещение учебных занятий и практики, консультаций.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	типовые методы и способы выполнения профессиональных задач.	организовывать собственную деятельность, оценивать эффективность и качество профессиональных задач.	-мотивированного обоснования выбора и применения методов и способов решения профессиональных задач. -точного, правильного и полного выполнения профессиональных задач. -разработки пользовательского интерфейса
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	основы нормативной в области разработки и эксплуатации программных продуктов.	принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	-демонстрации способности принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	перечень профессиональных задач и способы их эффективного решения.	осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	-обоснования выбора информационных источников для решения профессиональных задач. -оперативности поиска и использования необходимой информации для качественного выполнения профессиональных задач и личностного развития. -использования различных источников информации, включая электронные.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.	современное ПО для поддержки информационно-коммуникационных технологий	использовать информационно-коммуникационные технологии в профессиональной деятельности.	-осуществления операций с использованием общего и специализированного программного обеспечения. -создания отдельных компонент. -выполнения спецификаций компонент
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать	задачи профессионального и личностного развития.	заниматься самообразованием, осознанно планировать повышение квалификации.	-качественного, своевременного и полного выполнения заданий внеаудиторной самостоятельной работы. -обоснования постановки целей и задач самообразования. -планирования создания кода программного продукта на уровне

	повышение квалификации.			модуля.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	направления и перспективы развития технологий в области разработки и эксплуатации ПО.	ориентироваться в условиях частой смены технологий в профессиональной деятельности.	-анализа инноваций в области профессиональной деятельности; -отслеживания динамики развития языков программирования и средств его автоматизации.
ПК 1.1.	Выполнять разработку спецификаций отдельных компонент.	*сущность и понятие информационной безопасности, характеристику ее составляющих; безопасности;	*классифицировать защищаемую информацию по видам тайны и степеням конфиденциальност и;	проверки правил доступа к техническим и программным ресурсам компьютерной сети организации.
ПК 1.2.	Осуществлять разработку кода программного продукта на основе готовых спецификаций на уровне модуля.	*место информационной безопасности в системе национальной безопасности страны;	*применять основные правила и документы системы сертификации Российской Федерации;	установки антивирусного программного
ПК 2.3.	Решать вопросы администрирования базы данных.	*источники угроз информационной безопасности и меры по их предотвращению;	*классифицировать основные угрозы безопасности информации;	использования инструментальных средств проверки целостности данных
ПК 2.4.	Реализовывать методы и технологии защиты информации в базах данных.	*жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;	- своевременно пополнять антивирусные базы и соответствующее программное обеспечение.	проведения планового создания резервных копий критической информации
ПК 3.1.	Анализировать проектную и техническую документацию на уровне взаимодействия компонент программного обеспечения.	*современные средства и способы обеспечения информационной безопасности.	-определять фишинговые ссылки	проверки ПО на вирусы через Интернет.
ПК 3.4.	Осуществлять разработку тестовых наборов и тестовых сценариев.	-методы создания и тестирования отдельных компонент.	- тестировать программу в целом.	восстановления ОС к последнему устойчивому состоянию.
ПК 3.6.	Разрабатывать технологическую документацию.	-правила описания спецификаций компонент	- проверять документацию на уникальность.	Обновления антивирусных баз данных.

2.СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Учебная нагрузка (всего)	**90**
Аудиторные занятия (всего)	**60**
В том числе:	
занятия лекционного типа	**40**
практические занятия (практикумы)	**20**
лабораторные занятия	
Самостоятельная работа (всего)	**30**
в том числе:	
Самостоятельная внеаудиторная работа в виде домашних практических заданий, индивидуальных заданий, самостоятельного подбора и изучения дополнительного теоретического материала	**30**
Вид промежуточной аттестации (экзамен)	Экзамен
Общая трудоемкость час	**90**

2.2. Структура дисциплины:

Наименование разделов и тем		**Количество аудиторных часов**		**Самостоятельная работа студента (час)**
	Всего	**Теоретическое обучение**	**Практические и лабораторные занятия**	
Тема 1. Актуальность проблемы обеспечения информационной безопасности	**8**	**4**	**2**	**3**
Тема 2. Технические угрозы несанкционированного доступа и нарушения данных	**8**	**4**	**2**	**3**
Тема 3. Интеллектуальная собственность	**9**	**4**	**2**	**3**
Тема 4. Авторское право	**8**	**4**	**2**	**2**
Тема 5. Принципы политики безопасности	**8**	**4**	**2**	**3**
Тема 6. Программные средства защиты	**8**	**4**	**2**	**3**
Тема 7. Проблема вирусного заражения и структура современных вирусов	**8**	**4**	**2**	**3**
Тема 8. Защита от воздействия вирусов	**8**	**4**	**2**	**3**
Тема 9. Защита информационных систем	**8**	**4**	**2**	**3**

системами криптографии данных.				
Тема 10. Безопасное использование банковских карт.	**8**	**4**	**3**	**3**
Всего по дисциплине	**90**	**40**	**20**	**30**

2.3. Тематический план и содержание учебной дисциплины

ОП.11 Информационная безопасность

Наименование разделов и тем	**Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся**	**Объем часов**	**Уровень освоения**
1	**2**	**3**	**4**
Тема 1. Актуальность проблемы обеспечения информационной безопасности	Содержание учебного материала	***9***	
	Лекции. Основные понятия объекты, цели и задачи информационной безопасности. Основные понятия информационной безопасности.	4	*2*
	Практические занятия. Тема: Составление схемы информационных потоков на исследуемом объекте.	**2**	2
	Самостоятельная работа обучающихся: Рассмотреть действия и события, нарушающие информационную безопасность.	*3*	2
Тема 2. Технические угрозы несанкционированного доступа и нарушения данных	Содержание учебного материала	***9***	
	Лекции. Анализ технического состава сети и физическая защищенность информации.	4	*3*
	Практические занятия. Тема: Регламентация физического доступа к аппаратуре сети.	***2***	2
	Самостоятельная работа обучающихся: Исследование защиты аналогичных сетей.	3	2
Тема 3. Интеллектуальная собственность	Содержание учебного материала	***9***	
	Лекции. Понятие интеллектуальной собственности.	4	2
	Практические занятия. Тема: Предпринимательская деятельность в условиях рыночной экономики.	**2**	2
	Самостоятельная работа обучающихся: Необходимость защиты информации в современном мире	3	2
Тема 4.	Содержание учебного материала	**9**	

Авторское право	**Лекции.** Охрана авторского права законами государства	4	2
	Практические занятия. Законодательные акты.	**2**	2
	Самостоятельная работа обучающихся: Государственные стандарты защиты информации.	*3*	2
Тема 5. Принципы политики безопасности	Содержание учебного материала	***9***	
	Лекции. Виды политики безопасности. Уровни политики безопасности. Стратегии безопасности.	4	2
	Практические занятия. Тема: Роли и обязанности должностных лиц по разработке и внедрению политики безопасности.	***2***	2
	Самостоятельная работа обучающихся: Концепция системы безопасности предприятия. Правовой статус службы безопасности. Основные функции службы безопасности.	3	2
Тема 6. Программные средства защиты.	Содержание учебного материала	***9***	
	Лекции. Объекты и назначение программной защиты. Подходы к выбору средств защиты.	4	2
	Практические занятия. Тема: Программные средства защиты и борьбы с пиратством.	**2**	2
	Самостоятельная работа обучающихся: Ограничение доступа к компьютеру и операционной системе.	3	2
Тема 7. Проблема вирусного заражения и структура современных вирусов	Содержание учебного материала	**9**	
	Лекции. Общая характеристика компьютерных вирусов. Классификация компьютерных вирусов. Признаки проявления вирусов. Структура вирусов, пути их распространения.	4	2
	Практические занятия. Тема: Кейлоггеры. Классификация по типу, по месту хранения, по методу отправки и методу применения.	**2**	2
	Самостоятельная работа обучающихся: Подготовить презентацию на тему “Компьютерный вирус ”	3	2
Тема 8. Защита от воздействия вирусов	Содержание учебного материала	***9***	
	Лекции. Классификация методов защиты от компьютерных вирусов. Виды и назначение антивирусных программ.	4	2
	Практические занятия. Тема: Состав программного комплекса защиты от вирусов. Общая характеристика средств нейтрализации компьютерных вирусов.	**2**	2

	Самостоятельная работа обучающихся: Обзор современных антивирусных программ. Подготовить презентацию на тему “Антивирусная программа”.	3	2
Тема 9. Защита информационных систем системами криптографии данных	Содержание учебного материала	***9***	
	Лекции. Применение программных продуктов для защиты интеллектуальной собственности.	4	2
	Практические занятия. Тема: Программная защита интеллектуальной собственности.	**2**	2
	Самостоятельная работа обучающихся: Ролевое управление доступом в коммерческом банке.	*3*	2
Тема 10. Безопасное использование банковских карт.	Содержание учебного материала	***9***	
	Лекции. Физические и программные методы защиты взаимодействия с банковскими картами. Клиент-банк.	4	*2*
	Практические занятия. Тема: Хакерские атаки и методы защиты от них.	**2**	2
	Самостоятельная работа обучающихся: Технические средства борьбы с промышленным шпионажем.	*3*	2
Итого	Лекции	***40***	
	Практические занятия.	**20**	
	Самостоятельная работа обучающихся	30	
	Всего	**90**	

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

№ темы	Наименование темы	Содержание темы	Форма текущего контроля
1	2	3	4
1	Актуальность проблемы обеспечения информационной безопасности	Основные понятия объекты, цели и задачи информационной безопасности. Основные понятия информационной безопасности.	Т, У
2	Технические угрозы несанкционированного доступа и нарушения данных	Анализ технического состава сети и физическая защищенность информации.	Т, У
3	Интеллектуальная собственность	Понятие интеллектуальной собственности.	Т, У
4	Авторское право	Охрана авторского права законами государства	Т, У
5	Принципы политики безопасности	Виды политики безопасности. Уровни политики безопасности. Стратегии безопасности.	Т, У
6	Программные средства защиты	Объекты и назначение программной защиты. Подходы к выбору средств защиты.	Т, У
7	Проблема вирусного заражения и структура современных вирусов	Общая характеристика компьютерных вирусов. Классификация компьютерных вирусов. Признаки проявления вирусов. Структура вирусов, пути их распространения.	Т, У
8	Защита от воздействия вирусов	Классификация методов защиты от компьютерных вирусов. Виды и назначение антивирусных программ.	Т, У
9	Защита информационных систем системами криптографии данных.	Применение программных продуктов для защиты интеллектуальной собственности.	Т, У
10	Безопасное использование банковских карт.	Физические и программные методы защиты взаимодействия с банковскими картами. Клиент-банк.	Т, У
Примечание: Т – тестирование, У – устный опрос			

2.4.2. Занятия семинарского типа

 не предусмотрены

2.4.3. Практические занятия

№ темы	Наименование темы	Содержание темы	Форма текущего контроля

1	2	3	4
1	Актуальность проблемы обеспечения информационной безопасности	Составление схемы информационных потоков на исследуемом объекте.	Т, У
2	Технические угрозы несанкционированного доступа и нарушения данных	Регламентация физического доступа к аппаратуре сети.	Т, У
3	Интеллектуальная собственность	Предпринимательская деятельность в условиях рыночной экономики.	Т, У
4	Авторское право	Законодательные акты.	Т, У
5	Принципы политики безопасности	Роли и обязанности должностных лиц по разработке и внедрению политики безопасности.	Т, У
6	Программные средства защиты	Программные средства защиты и борьбы с пиратством.	Т, У
7	Проблема вирусного заражения и структура современных вирусов	Кейлоггеры. Классификация по типу, по месту хранения, по методу отправки и методу применения.	Т, У
8	Защита от воздействия вирусов	Состав программного комплекса защиты от вирусов. Общая характеристика средств нейтрализации компьютерных вирусов.	Т, У
9	Защита информационных систем системами криптографии данных.	Программная защита интеллектуальной собственности.	Т, У
10	Безопасное использование банковских карт.	Хакерские атаки и методы защиты от них.	Т, У
Примечание: Т – тестирование, У – устный опрос			

2.4.4. Содержание самостоятельной работы

На самостоятельную работу студентов отводится 20 часов учебного времени.

№	Наименование темы, вида СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	Актуальность проблемы обеспечения информационной безопасности	1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. - М.: ФОРУМ: ИНФРА-М.- 2016.- 415 с. 2. Партыка, Т.Л. Информационная безопасность: учеб. пособие для СПО /Т.Л. Партыка, И.И. Попов. -5-е изд., перераб. и доп.- М.:ФОРУМ,2014.-431 с. 3. *Нестеров, С. А.* Информационная безопасность [Электронный ресурс]: учебник и практикум / С. А. Нестеров. — М.: Издательство Юрайт, 2017. — 321 с. - URL: https://www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7 4. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник / О.В. . - Самара: Самарский государственный архитектурно-строительный университет, 2014. - 113 с. - URL: http://biblioclub.ru/index.php?page=book_red&id=438331&sr=1 5. Зайцев, А.П. Технические средства и методы защиты
2	Технические угрозы несанкционированного доступа и нарушения данных	
3	Интеллектуальная собственность	
4	Авторское право	
5	Принципы политики безопасности	
6	Программные средства защиты	
7	Проблема вирусного	

	заражения и структура современных вирусов	информации: учебник /А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов.- М.: Горячая линия-Телеком, 2014.-442с. 6. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / С.А. Нестеров. - СПб.: Издательство Политехнического университета, 2014. - 322 с. - URL: http://biblioclub.ru/index.php?page=book_red&id=363040&sr=1
8	Защита от воздействия вирусов	
9	Защита информационных систем системами криптографии данных.	
10	Безопасное использование банковских карт.	

Кроме перечисленных источников студент может воспользоваться поисковыми системами сети Интернет по теме самостоятельной работы.

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

Самостоятельная работа студентов является важнейшей формой учебно-познавательного процесса.

Основная цель самостоятельной работы студента при изучении дисциплины – закрепить теоретические знания, полученные в ход лекционных занятий, а также сформировать практические навыки подготовки в области программирования.

Самостоятельная работа студента в процессе освоения дисциплины включает:

-изучение основной и дополнительной литературы по курсу;

-самостоятельное изучение некоторых вопросов (конспектирование);

-работу с электронными учебными ресурсами;

-изучение материалов периодической печати, интернет ресурсов;

-подготовку к тестированию;

-подготовку к практическим занятиям,

-самостоятельное выполнение домашних заданий.

Для помощи в самостоятельной работе рекомендуется применять электронный учебник (учебное пособие) **Программирование.CHM**, разработанное Левиным Л.Л.

Для освоения данной дисциплины и выполнения предусмотренных учебной программой курса заданий по самостоятельной работе студент может использовать следующее учебно-методическое обеспечение:

-обучающие видеофильмы и программы по тематике решаемых задач из **Видеотеки программирования** филиала (225 единиц);

-программу компьютерного обучения и контроля “**ЭкзамL**”;

-электронный учебник по прикладному программированию;

-методические рекомендации преподавателя к лекционному материалу;

-методические рекомендации преподавателя к практическим занятиям;

-методические рекомендации преподавателя к выполнению самостоятельных домашних заданий.

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. Студент должен уметь пользоваться фондами библиотек и справочно-библиографическими изданиями.

Студенты для полноценного освоения учебного курса должны составлять конспекты как при прослушивании его теоретической (лекционной) части, так и при подготовке к практическим (лабораторным) занятиям. Желательно, чтобы конспекты лекций записывались в логической последовательности изучения курса и содержались в одной тетради.

3. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для реализации компетентностного подхода предусматривается использование в учебном процессе компьютерных активных и интерактивных форм проведения аудиторных и внеаудиторных занятий с целью формирования и развития профессиональных навыков обучающихся.

В процессе преподавания применяются образовательные технологии развития критического мышления. Обязательны компьютерные практические работы по разделам дисциплины.

В учебном процессе наряду с традиционными образовательными технологиями используются электронные учебники, компьютерное обучение, тестирование, учебные видеофильмы, тематические презентации, интерактивные технологии.

3.1. Образовательные технологии при проведении лекций

№	Тема	Виды применяемых образовательных технологий	Кол-во час
1	2	3	4
1	Актуальность проблемы обеспечения информационной	Компьютерные технологии обучения, активное обучение, электронный учебник, тестирование.	4*
2	Технические угрозы несанкционированного доступа и		4*
3	Интеллектуальная собственность		4*
4	Авторское право		4*
5	Принципы политики безопасности		4*
6	Программные средства защиты		4*
7	Проблема вирусного заражения и структура		4*
8	Защита от воздействия вирусов		4*
9	Защита информационных систем системами		4*
10	Безопасное использование банковских карт.		4*
	Итого по курсу		40
	в том числе интерактивное обучение*		40*

3.2.Образовательные технологии при проведении практических занятий

№	Тема занятия	Кол. час	Виды применяемых образовательных технологий
1	Составление схемы информационных потоков на исследуемом объекте.	2*	Компьютерные технологии обучения. Электронный учебник. Активное обучение. Дискуссия по теоретическим вопросам. Решение задач индивидуально.
2	Регламентация физического доступа к аппаратуре сети.	2*	
3	Предпринимательская деятельность в условиях рыночной экономики.	2*	
4	Законодательные акты.	2*	
5	Роли и обязанности должностных лиц по разработке и внедрению политики безопасности.	2*	

6	Программные средства защиты и борьбы с пиратством.	**2***	Решение задач малыми группами. Разбор решения задач.
7	Кейлоггеры. Классификация по типу, по месту хранения, по методу отправки и методу применения.	**2***	
8	Состав программного комплекса защиты от вирусов. Общая характеристика средств нейтрализации компьютерных вирусов.	**2***	
9	Программная защита интеллектуальной собственности.	**2***	
10	Хакерские атаки и методы защиты от них.	**2***	
	Итого по курсу	20	
	в том числе интерактивное обучение*	20*	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

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

Реализация учебной дисциплины осуществляется в специально оборудованном компьютерном классе.

Оборудование учебного кабинета:

- мультимедийный проектор, экран;
- персональный компьютер, динамики;
- выход в Интернет;
- учебная мебель;
- доска учебная;

Наглядные пособия:

1. Видеофильм Архивация данных.webm
2. Видеофильм Классификация ПО.mp4
3. Видеофильм Безопасность информационных систем Карпов.mp4
4. Видеофильм Система управления БД OpenOffice.mp4
5. Видеофильм Локальные компьютерные сети.mp4
6. Видеофильм Объекты операционной системы.mp4
7. Видеофильм Файлы. Файловая система.mp4

Электронные ресурсы:

1. Технология разработки прикладного программного обеспечения https://www.monographies.ru/ru/book/view?id=141
2. Справочник Delphi http://delphimaster.net/ Delphi Master Search Archive
3. Учебник Delphi http://www.delphi-manual.ru/ Уроки Delphi начинающим с нуля
4. Delphi компоненты. Справочник http://www.delphisources.ru/
5. Delphi Форум программистов http://www.programmersforum.ru/index.php
6. Он-лайн справочник. Основы Delphi http://www.delphibasics.ru/

4.2. Перечень необходимого программного обеспечения

1. Kaspersky Anti-Virus. URL https://www.kaspersky.ru/ (в свободном доступе);
2. Avast Internet Security URL https://www.avast.ru/internet-security. (в свободном доступе);
3. Lazarus – визуальная среда программирования (в свободном доступе);
4. PascalABC - визуальная среда программирования (в свободном доступе);
5. PascalABC.NET - визуальная среда программирования (в свободном доступе);
6. ESET NOD32 Internet Security https://www.esetnod32.ru (в свободном доступе);
7. 7-zip архиватор; (лицензия на англ. http://www.7-zip.org/license.txt)
8. Adobe Acrobat Reader просмотрщик файлов ; (лицензия - https://get.adobe.com/reader/?loc=ru&promoid=KLXME)
9. Adobe Flash Player –графический редактор; (лицензия - https://get.adobe.com/reader/?loc=ru&promoid=KLXME)
10. Apache OpenOffice – офисный пакет; (лицензия - http://www.openoffice.org/license.html)
11. FreeCommander - проводник; (лицензия - https://freecommander.com/ru/%d0%bb%d0%b8%d1%86%d0%b5%d0%bd%d0%b7%d0%b8%d1%8f/)
12. Google Chrome - браузер;(лицензия - https://www.google.ru/chrome/browser/privacy/eula_text.html)
13. LibreOffice – офисный пакет (в свободном доступе);
14. Mozilla Firefox - браузер.(лицензия - https://www.mozilla.org/en-US/MPL/2.0/)
15. nanoCAD версия 5.1 локальная (лицензия - серийный номер: NC50B-45103)
16. ЭкзамL – Система компьютерного тестирования http://Lkub.ru Левин Л.Л. (в свободном доступе);
17. Программный комплекс "Универсальный тест 4.0.0.1" http://www.timk.ru/ (в свободном доступе);

5. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОП.11 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

5.1. Основная литература

1. Нестеров, С. А. Информационная безопасность [Электронный ресурс]: учебник и практикум / С. А. Нестеров. — М.: Издательство Юрайт, 2017. — 321 с. - URL: https://www.biblio-online.ru/viewer/836C32FD-678E-4B11-8BFC-F16354A8AFC7#page/1

5.2. Дополнительная литература

1. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. - М.: ФОРУМ: ИНФРА-М.- 2016.- 415 с. 5
2. Партыка, Т.Л. Информационная безопасность: учеб. пособие для СПО /Т.Л. Партыка, И.И. Попов. -5-е изд., перераб. и доп.- М.:ФОРУМ,2014.- 431 с. 5
3. Зайцев, А.П. Технические средства и методы защиты информации: учебник /А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов.- М.: Горячая линия-Телеком, 2014.-442с. 4
4. Внуков, А. А. Защита информации в банковских системах [Электронный ресурс]: учебное пособие / А. А. Внуков. — 2-е изд., испр. и доп. — М.: Издательство Юрайт, 2017. — 246 с. - URL: https://www.biblio-online.ru/viewer/2095B353-8AE3-4A0F-987F-00C157F3BDE7#page/1
5. Внуков, А. А. Защита информации [Электронный ресурс]: учебное пособие / А. А. Внуков. — 2-е изд., испр. и доп. — М.: Издательство Юрайт, 2017. — 261 с. - URL: https://www.biblio-online.ru/viewer/73BEF88E-FC6D-494A-821C-D213E1A984E1#page/1
6. Лось, А. Б. Криптографические методы защиты информации [Электронный ресурс]: учебник / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М.: Издательство Юрайт, 2017. — 473 с. - URL: https://www.biblio-online.ru/viewer/27397D56-C8A1-4970-9F39-28E7FA40632A#page/1
7. Запечников, С. В. Криптографические методы защиты информации [Электронный ресурс]: учебник / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — М.: Издательство Юрайт, 2017. — 309 с. - URL: https://www.biblio-online.ru/viewer/B27D8A2B-F86C-4F18-9F21-3E0695C0A4C0#page/1
8. Нетёсова, О. Ю. Информационные технологии в экономике [Электронный ресурс]: учебное пособие для СПО / О. Ю. Нетёсова. — 3-е изд., испр. и доп. — М.: Издательство Юрайт, 2017. — 146 с. - URL:

https://www.biblio-online.ru/viewer/D8F3F1FA-DA19-468F-A7FD-73E7BD1ACDCC#page/1
9. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебник и практикум для СПО / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; отв. ред. Т. А. Полякова, А. А. Стрельцов. — М.: Издательство Юрайт, 2017. — 325 с. - URL: https://www.biblio-online.ru/viewer/054509D0-1E35-4080-9E86-19742B336897#page/1
10. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты [Электронный ресурс]: учебник / В. М. Фомичёв, Д. А. Мельников ; под ред. В. М. Фомичёва. — М.: Издательство Юрайт, 2017. — 209 с. - URL: https://www.biblio-online.ru/viewer/C0328DC2-2A46-4945-994F-04F661095B83#page/1
11. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты [Электронный ресурс]: учебник / В. М. Фомичёв, Д. А. Мельников ; под ред. В. М. Фомичёва. — М.: Издательство Юрайт, 2017. — 245 с. - URL: https://www.biblio-online.ru/viewer/AF99BBDE-AF3A-43A9-A90F-B99806553C25#page/1
12. Васильева, И. Н. Криптографические методы защиты информации [Электронный ресурс]: учебник и практикум / И. Н. Васильева. — М.: Издательство Юрайт, 2017. — 349 с. - URL: https://www.biblio-online.ru/viewer/59BABD78-5536-4ED4-BB9D-55E2F19F80B2#page/1

5.3 Периодические издания

1. Среднее и профессиональное образование
2. Компьютер Пресс
3. Открытые системы.- URL: http://biblioclub.ru/index.php?page=journal&jid=436083
4. Информатика в школе .- URL: http://dlib.eastview.com/browse/publication/18988
5. Программные продукты и системы.- URL: http://dlib.eastview.com/browse/publication/64086
6. Информатика и образование.- URL: http://dlib.eastview.com/browse/publication/18946
7. Системный администратор.- URL: http://dlib.eastview.com/browse/publication/66751
8. Computerword Россия.- URL: http://dlib.eastview.com/browse/publication/64081
9. Мир ПК.- URL: http://dlib.eastview.com/browse/publication/64067
10. 10.Информационно-управляющие системы.- URL: http://dlib.eastview.com/browse/publication/71235
11. Журнал сетевых решений LAN.- URL: http://dlib.eastview.com/browse/publication/64078

12. Информатика и образование.- URL: http://dlib.eastview.com/browse/publication/18946
13. Windows IT Pro/ Re.- URL: http://biblioclub.ru/index.php?page=journal&jid=138741
14. Прикладная информатика.- URL: http://elibrary.ru/title_about.asp?id=25599

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

1. ЭБС «Университетская библиотека ONLINE». – URL: www.biblioclub.ru
2. ЭБС издательства «Лань». – URL: https://e.lanbook.com
3. ЭБС «Юрайт». – URL: http://www.biblio-online.ru/
4. Электронный каталог Научной библиотеки КубГУ. – URL:http://212.192.134.46/MegaPro/Catalog/Home/Index
5. Электронная библиотека «Издательского дома «Гребенников» - URL:www.grebennikon.ru
6. Научная электронная библиотека (НЭБ) «eLibrary.ru». - URL:http://www.elibrary.ru
7. Базы данных компании «Ист Вью». - URL:http://dlib.eastview.com
8. Лекториум ТВ». - URL: http://www.lektorium.tv/
9. Национальная электронная библиотека «НЭБ». - URL:http://нэб.рф/
10. КиберЛенинка: научная электронная библиотека. – URL: http://cyberleninka.ru/
11. Единое окно доступа к образовательным ресурсам : федеральная ИС свободного доступа. – URL: http://window.edu.ru.
12. Справочно-правовая система «Консультант Плюс» - URL http://www.consultant.ru

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по выполнению практических работ

Перечень практических заданий

Задание 1 Разработать функциональную модель декомпозиции учета движения материалов на складе фирмы

Задание 2 Разработать функциональную модель работы информационной системы приемной комиссии института

Задание 3 Разработать функциональную модель декомпозиции работы информационно-справочной службы фирмы

Задание 4 Разработать функциональную модель работы информационной системы городского бюро медико-социальной экспертизы

Задание 5 Разработать функциональную модель декомпозиции работы информационной системы туристической фирмы

Задание 6 Разработать функциональную модель работы офиса продаж оператора сотовой связи

Задание 7 Разработать функциональную модель декомпозиции работы бухгалтерии предприятия

Задание 8 Разработать функциональную модель работы переговорного пункта

Задание 9 Разработать функциональную модель декомпозиции работы регистратуры больницы

Задание 10 Разработать функциональную модель декомпозиции работы отдела кадров предприятия

Задание 11 Разработать функциональную модель работы учебного отдела вуза

Задание 12 Разработать функциональную модель декомпозиции работы деканата СПО

Задание 13 Разработать модель информационной системы страховой компании

Задание 14 Разработать модель информационной системы пункта проката видеофильмов

Задание 15 Разработать модель информационной системы начисления сдельной заработной платы

Задание 16 Разработать модель информационной системы учета транспортных перевозок

Задание 17 Разработать модель информационной системы кассы автостанции

Задание 18 Разработать в модель информационной системы учета заявок клиентов торговой фирмы

К задаче указать критические места возможной утечки и разрушения информации.

7. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ УСПЕВАЕМОСТИ

7.1. Паспорт фонда оценочных средств

Код и наименование элемента **знаний,** контролируемые компетенции

З1	сущность и понятие информационной безопасности, характеристику ее составляющих;	ПК 1.1
З2	место информационной безопасности в системе национальной безопасности страны;	ПК 1.2
З3	источники угроз информационной безопасности и меры по их предотвращению;	ПК 2.3
З4	жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;	ПК 2.4
З5	современные средства и способы обеспечения информационной безопасности;	ПК 3.1

Код и наименование элемента **умений,** контролируемые компетенции

У1	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;	ПК 3.4, ПК 3.6
У2	применять основные правила и документы системы сертификации Российской Федерации;	ПК 1.2
У3	классифицировать основные угрозы безопасности информации;	ПК 2.3

Для оценки вышеуказанных знаний и умений используются программы, разработанные и отлаженные обучающимся, которые представлены преподавателю. Дополнительный контроль проводится с помощью тематических тестов и собеседований.

7.2. Критерии оценки знаний

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных самостоятельных заданий и курсовых работ.

Курсовая работа. Продукт самостоятельной работы студента, представляющий собой разработанную блок-схему алгоритма решения задачи и компьютерную программу, реализующую алгоритм на языке Dephi. Прилагаются результаты отладки и тестирования программы. Программа оценивается по степени выполнения технического задания, правильности работы, дружественности интерфейса, разнообразию применённых компонент, времени изготовления программы и степени оригинальности решений.

Тест. Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Тест оценивается по количеству правильных ответов, по времени выполнения, весу (сложности) заданий (не менее 50%).

Критерии оценки знаний студентов в целом по дисциплине:

«отлично» - выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений;

«хорошо» - выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности;

«удовлетворительно» - выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации;

«неудовлетворительно» - выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач.

7.3. Оценочные средств для проведения текущей аттестации

В данном разделе приводятся образцы оценочных средств. Полный комплект оценочных средств имеется в Фонде оценочных средств.

Текущий контроль проводится в форме:

-тестирование по теоретическому и практическому материалу

-практическая работа – разработка и отладка программы

-защита выполненного задания,

-индивидуальный устный опрос.

Форма аттестации	Знания	Умения	Практический опыт (владение)	Личные качества студента	Примеры оценочных средств
Устный (письменный) опрос по темам	Контроль знаний по закладкам Delphi с встроенными компонентами	Оценка умения применять компоненты для разработки программ	Оценка навыков разработки законченных программ	Оценка способности оперативно и качественно отвечать на поставленные вопросы	Контрольные вопросы по темам прилагаются
Практические работы	Контроль знания основ программирования свойств и событий компонент Delphi	Оценка умения работать с графическими компонентами Delphi	Оценка навыков работы прикладными программными средствами	Оценка способности качественно решать задачи и аргументировать результаты	Темы работ прилагаются
Тестирование	Контроль знаний по определенным темам	Оценка умения различать конкретные понятия алгоритмов	Оценка навыков логического анализа и синтеза при сопоставлении конкретных понятий	Оценка способности оперативно и качественно отвечать на поставленные вопросы	Вопросы прилагаются

Балльно-рейтинговая система контроля

В основу фиксирования достижений учащихся положена компьютерная программа «**Рейтинг-автомат**», разработанная Левиным Л.Л., в которой имеются две главные связанные таблицы: 1. Список студентов по горизонтали и по вертикали Дата/Код КИМ/Сложность (вес) КИМ. 2. Список кодов тем занятий (КИМ) и содержание. При заполнении таблиц происходит автоматический пересчет баллов, набранных каждым студентом, ранжирование списка по набранным баллам, печать индивидуальных экзаменационных билетов с перечислением тем, пропущенных студентом. За посещение студентом занятия ему начисляется 1 балл. В качестве КИМ в значительной степени используются различные компьютерные тестовые системы, набранные баллы из которых заносятся в первую таблицу. Сложность КИМ назначает преподаватель.

Для текущего и итогового контроля применяется компьютерная программа «**ЭкзамL**», разработанная Левиным Л.Л. для компьютерного контроля и тестирования, работающая в режиме обучения и контроля. Характеристики тем, заложенных в программу, приведены ниже.

1. Windows Файловая система 51 вопрос
2. Excel Word Windows основы применения 54 вопроса
3. PowerPoint. Создание презентаций 30 вопросов
4. Архитектура ЭВМ, ОС, вирусы 61 вопрос
5. Архитектура компьютера 50 вопросов
6. Информация и информационные процессы Основы 23 вопроса
7. Информационная безопасность 79 вопросов
8. Информационная безопасность и Антивирусы 52 вопроса
9. Информационные технологии в образовании 100 вопросов
10. Сети компьютерные Аппаратные средства 60 вопросов
11. Сети компьютерные, телекоммуникации, Интернет 46 вопросов
12. Операционные системы, среды и оболочки 95 вопросов
13. Технические средства информатизации 22 вопроса
14. Инфокоммуникационные системы и сети 100 вопросов

Список других программ для обучения и тестирования студентов
Список программ для компьютерной проверки знаний, используемых в СПО КубГУ

ФЗ-149 аттестация системных администраторов

- тест предназначен для аттестации системных администраторов (знание законов и нормативных актов, регулирующих профессиональную деятельность сотрудника). Тематика теста: №149-ФЗ "Об информации, информационных технологиях и о защите информации".

Автор теста Лисичкин А.А. Должность: главный специалист (системный администратор). Место работы: Минздравсоцразвития РФ.

ФЗ-149 аттестация системных администраторов

Информационная безопасность

- тест содержит вопросы по методам и средствам защиты информации для студентов 4-го курса ЮРГТУ (101 вопрос).

Автор теста: ст. преподаватель ЮРГТУ Максименко М.В.

Безопасность в интернете

- тест "Безопасность в интернете" (45 вопросов).

Автор теста: Квашнин М.Г, создан на базе теста «Информационной безопасность» ст. преподавателя ЮРГТУ Максименко М.В.

7.4. Оценочные средств для проведения промежуточной аттестации

Промежуточная аттестация

Форма аттестации	Знания	Умения	Иметь практический опыт	Личные качества студента	Примеры оценочных средств
Экзамен/диф зачет, тест по теме, комплексный тест по предметам	Контроль знания базовых положений в прикладном программировании	Оценка умения понимать специальную терминологию	Оценка навыков логического анализа задачи придумывать алгоритм.	Оценка способности грамотно и четко излагать материал	Вопросы: прилагаются
		Оценка умения разрабатывать алгоритмы и писать программы на языках высокого уровня.	Оценка навыков Переработки алгоритма в компьютерную программу	Оценка способности грамотно и четко излагать ход работы программы и аргументировать результаты	Задачи прилагаются

7.4.1. Примерные вопросы для проведения промежуточной аттестации

Практическая работа №1 Защита информации от копирования: задание некопируемых меток
Практическая работа №2 Защита программ от дисассемблирования.
Практическая работа №3. Защита программ в оперативной памяти.
Практическая работа №4. Защита программ в оперативной памяти.
Практическая работа №5. Приемы работы с защищенными программами.
Самостоятельная работа №1. Защита информации от копирования: задание некопируемых меток
Самостоятельная работа №2. Защита программ от дисассемблирования.
Самостоятельная работа №3. Защита программ в оперативной памяти.
Самостоятельная работа №4. Защита программ в оперативной памяти.
Самостоятельная работа №5. Приемы работы с защищенными программами.

7.4.2. Примерные экзаменационные задачи

Практическая работа №1. Перехват вывода на экран
Практическая работа №2. Перехват вывода на экран
Практическая работа №3. Перехват ввода с клавиатуры
Практическая работа №4. Перехват и обработка файловых операций
Практическая работа №5. Особенности закладок и защита от воздействия закладок
Самостоятельная работа №1. Перехват вывода на экран
Самостоятельная работа №2. Перехват ввода с клавиатуры
Самостоятельная работа №3. Перехват и обработка файловых операций
Самостоятельная работа №4. Особенности закладок и защита от воздействия закладок
Самостоятельная работа №5. Пакеты антивирусных программ

Вопросы к экзамену

1. Информационная безопасность. Безопасность информации. Угрозы безопасности.
2. Меры противодействия угрозам безопасности.
3. Формальные модели безопасности. Дискреционная, мандатная, ролевая.
4. Методы аутентификации. Методы определения паролей.
5. Парольная аутентификация, хэш-функции.
6. Парольные взломщики. Стойкость паролей.
7. Методы надёжного удаления информации.
8. Межсетевые экраны.
9. Методы защиты конфиденциальности. Стеганографические методы защиты информации. Компьютерная стеганография

Контрольная работа по дисциплине "**Информационная безопасность**" является итоговой формой контроля знаний студентов, самостоятельной работой студентов на завершающем этапе изучения данной дисциплины.

Цель контрольной работы - закрепление теоретических знаний по курсу, получение практических навыков составления бизнес-плана.

Контрольная работа представляет собой разработанный студентом алгоритм и написание программы для выбранной задачи.

Объем контрольной работы - 5-10 стр.; время, отводимое на подготовку – от 2 недель до месяца.

Работа должна состоять из следующих частей:

- Постановка задачи.
- Описание алгоритма решения.
- Блок-схема алгоритмы.
- Текст программы на языке Паскаль.

- Описание встретившихся проблем и ошибок.
- Демонстрация на компьютере работающей программы.
- Описание возможных усовершенствований программы.
- Приложения (если необходимо).

В приложениях помещаются по необходимости иллюстрированные материалы, имеющие вспомогательное значение (схемы, диаграммы и т.п.).

Выполненная контрольная работа проверяется преподавателем, затем защищается студентом и оценивается в форме зачета и экзамена.

8. ДОПОЛНИТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приложение 1. Краткий конспект лекционных занятий

Тема 1. Понятие интеллектуальной собственности. Предпринимательская деятельность в условиях рыночной экономики. Необходимость защиты информации в современном мире.

Тема 2. Авторское право. Охрана авторского права законами государства . Законодательные акты. Государственные стандарты защиты информации.

Авторское право. Объекты авторского права. Субъекты авторского права. Соавторство. Законодательные акты. Компьютерная информация как объект правовой защиты. Общая характеристика преступлений в компьютерной сфере по современному Российскому уголовному законодательству

Тема 3. Принципы политики безопасности. [Виды политики безопасности. Уровни политики безопасности. Стратегии безопасности. Роли и обязанности должностных лиц по разработке и внедрению политики безопасности.

Что должно быть содержанием политики безопасности. Получение разрешения. Претворение политики в жизнь. Некоторые замечания по поводу политики. Примеры описания общих принципов работы в Интернете в политиках

Тема 4. Концепция системы безопасности предприятия. Правовой статус службы безопасности. Основные функции службы безопасности .

Концепция безопасности предприятия. Правовой статус службы безопасности. Недобросовестная конкуренция. Основные функции службы безопасности

Тема 5. Каналы утечки информации. Технические средства борьбы с промышленным шпионажем.

Методы и средства блокирования

Тема 6. Программные средства защиты. Объекты и назначение программной защиты. Подходы к выбору средств защиты.

Средства обеспечения безопасности компьютерных сетей. Средства анализа защищенности сетевых сервисов (служб). Средства анализа защищенности операционных систем. Средства анализа защищенности приложений. SWIFT система телекоммуникационного обслуживания для банков. Электронные системы межбанковских расчетов. Механизмы и средства защиты сетей. Анализ защищенности. Обзор средств анализа защищенности

Тема 7. Программные средства защиты и борьбы с пиратством. Ограничение доступа к компьютеру и операционной системе.

Программные средства с криптографической зашитой конфиденциальной информации от несанкционированного доступа. Всестороннее ограничение доступа к компьютеру и ОС

Тема 8. Защита информационных систем системами криптографии данных. Программная защита интеллектуальной собственности. Ролевое управление доступом в коммерческом банке.

Система передачи зашифрованных сообщений в режиме реального времени на базе виртуальной одноранговой сети. Ролевое управление доступом

Тема 9. Применение программных продуктов для защиты интеллектуальной собственности. Примеры программных продуктов. Хакерские атаки и методы защиты от них.

Система обнаружения атак RealSecure. Хакерская атака. Типичные атаки. Атаки на доверие. Комплексный подход к защите

Тема 10. Резервное копирование данных и архивация. План копирования и восстановления данных.

Приложение 2. Презентации.

Папка F:\Uni\2017_18\14П\Информационная безопасность\РП\2017\Лекции Презентации На 30.08.2017

№	Имя файла	Байт	Дата
1	Безопасность данных и информационная защита.pptx	391904	05.09.2017
2	Безопасный интернет детям.pdf	6449390	25.08.2016
3	Буклет ФЗ436.doc	215552	25.08.2016
4	Информационная безопасность.pptx	967959	26.08.2016
5	Карта банка.pdf	1478547	26.03.2012
6	Лекция	Папка	21.02.2015

ЛИСТ
изменений рабочей учебной программы по дисциплине
ОП.11 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Дополнения и изменения, вносимые в рабочую программу дисциплины

Основания внесения дополнений и изменений	Раздел РПД, в который вносятся изменения	Содержание вносимых дополнений, изменений
Предложение работодателя		
Предложение составителя программы		
Другие основания		

Составитель: преподаватель _____ Л.Л. Левин канд.техн.наук
подпись

Утверждена на заседании предметной (цикловой) комиссии профессиональных дисциплин программирования и компьютерных протокол № 1 от «31» августа 2017 г.

Председатель предметной (цикловой) комиссии профессиональных дисциплин программирования в компьютерных системах _____ Л.А. Благова
«31» августа 2017 г.

Зам. директора по УР филиала _____ Т. А. Резуненко
«31» августа 2017г.

Заведующая сектором библиотеки _____ Л. Г. Соколова
«31» августа 2017г.

Инженер-электроник (программно-информационное обеспечение образовательной программы) _____ А. В. Сметанин
«31» августа 2017г.

РЕЦЕНЗИЯ

на рабочую программу по учебной дисциплине **МДК 02.03. «Информационная безопасность»** по специальности 09.02.03 «Программирование в компьютерных системах» СПО, разработанную кандидатом технических наук, преподавателем **Левиным Львом Львовичем.**

По структуре программа соответствует современному уровню развития технологий защиты информации и компьютерной техники, она включает в себя описание актуальных угроз и средств борьбы с ними, как программно-алгоритмических так и технических.

Рабочая программа предусматривает освоение профессиональных компетенций: (ПК1.1. ПК1.2. ПК2.3. ПК2.4. ПК3.1. ПК3.4. ПК3.6.) и видов деятельности, согласно ФГОС 09.02.03 Программирование в компьютерных системах, приказ Минобрнауки РФ от 28.07.2014 №804.

В рабочую программу включено изучение организационных, технических и программных средств защиты информации, анализ антивирусного ПО, типов угроз, особенности хищения, подмены и уничтожения информации, необходимого инструментария. Программа имеет достаточную степень полноты и законченности изучения предмета.

Дисциплина «Информационная безопасность» предусматривает приобретение навыков в установки антивирусного программного обеспечения, противодействия попыткам взлома и несанкционированного доступа к защищаемой информации, фишинга и блокировки данных.

В рабочей программе нашли отражение важные примеры признаков заражения компьютера, способы профилактики и борьбы с последствиями атак, что даёт возможность и умение решать конкретные задачи по защите информации с использованием имеющихся инструментов.

Структура программы соответствует современным требованиям. Содержание каждого её элемента проработано с достаточной степенью полноты и законченности. Пояснительная записка раскрывает цели программы, включает в себя характеристику её предметного содержания.

В программе приводится необходимый список учебных пособий.

Отметим также применение в учебном процессе балльно- рейтинговой системы оценивания знаний и программ тестирования.

В целом рецензируемая программа учебной дисциплины заслуживает положительной оценки, она достаточно продумана и ориентирована на подготовку обучающихся к использованию полученных навыков в своей профессиональной деятельности.

Таким образом, рабочая программа содержит все необходимые элементы рекомендуемой структуры, обладает достаточной полнотой и законченностью, является полезным практическим документом при преподавании дисциплины «Информационная безопасность».

Рецензент: Приходько Леонид Васильевич, директор ООО «ТКМ»

РЕЦЕНЗИЯ

на рабочую программу по учебной дисциплине

ОП.11 «**Информационная безопасность**» по специальности **09.02.03 «Программирование в компьютерных системах» СПО**, разработанную кандидатом техн. наук, преподавателем Левиным Львом Львовичем.

Содержание программы согласуется с современным состоянием развития технологий защиты информации и компьютерной техники, оно включает в себя описание актуальных угроз и средств борьбы с ними, как технических так и программно-алгоритмических.

Рабочая программа предусматривает освоение профессиональных компетенций: (ПК1.1. ПК1.2. ПК2.3. ПК2.4. ПК3.1. ПК3.4. ПК3.6.) и видов деятельности, согласно ФГОС 09.02.03 Программирование в компьютерных системах, приказ Минобрнауки РФ от 28.07.2014 №804.

В программу включено изучение организационных, технических и программных средств защиты информации, анализ антивирусного ПО, типов угроз, особенности хищения, подмены и уничтожения информации, необходимого инструментария.

Указанная дисциплина «Информационная безопасность» предусматривает приобретение навыков в установки антивирусных программ, противодействия попыткам взлома и несанкционированного доступа к защищаемой информации, блокировки данных и фишинга.

В рабочей программе отражены важные примеры признаков заражения компьютера, способы профилактики и борьбы с последствиями атак, что даёт возможность и умение решать конкретные задачи по защите информации с использованием имеющихся инструментов.

Структура программы соответствует современным требованиям. Содержание каждого её элемента разработано с достаточной степенью полноты и законченности. Пояснительная записка раскрывает ведущие цели программы, включает в себя краткую характеристику её предметного содержания.

Программа содержит необходимый список учебных пособий.

Следует отметить применение в учебном процессе балльно- рейтинговой системы оценивания знаний и программ тестирования.

Рецензируемая программа учебной дисциплины в целом заслуживает положительной оценки, она достаточно продумана и ориентирована на подготовку обучающихся к использованию полученных знаний и навыков в своей профессиональной деятельности.

Следовательно, рабочая программа содержит все необходимые элементы рекомендуемой структуры, обладает достаточной полнотой и законченностью, является полезным практическим документом при преподавании дисциплины «Информационная безопасность».

Рецензент: Брызгалов Олег Владимирович, ООО «Информационные системы и компьютерные технологии», заместитель директора