МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

математического анализа

Баев А.Д.

30.06.2017

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОГРАММЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ СРЕДНЕГО ЗВЕНА

ОП.09 Информационная безопасность

Код и наименование дисциплины в соответствии с Учебным планом
09.02.03 Программирование в компьютерных системах

Код и наименование специальности
технический

Профиль подготовки (технический, естественнонаучный, социально-экономический, гуманитарный)
техник-программист

Квалификация выпускника
очная

Форма обучения

Учебный год: 2019-2020 Семестр(ы): *6,7*

Рекомендована: Научно-методическим советом математического факультета
протокол от 26.06.2017 № 0500-06

Составители ФОС: Костин Алексей Владимирович, доцент кафедры математического моделирования, кандидат физико-математических наук

2017 г.

ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

ОП.09 Информационная безопасность

Фонд оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования (ФГОС СПО) по специальности 09.02.03 Программирование в компьютерных системах, утвержденного приказом Министерства образования и науки Российской Федерации **от 28 июля 2014 г. N 804** "Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.03 Программирование в компьютерных системах" и в соответствии с рабочей программой учебной дисциплины ОП.09 Информационная безопасность.

ФОС включает контрольные материалы для проведения текущей аттестации в виде контрольной работы и промежуточной аттестации в форме экзамена.

ФОС разработаны на основании положения: П ВГУ 2.2.01 – 2015 Положение о порядке организации и осуществления образовательной деятельности, текущей, промежуточной и итоговой аттестации по основным профессиональным образовательным программам среднего профессионального образования в Воронежском государственном университете.

1. Цели и задачи учебной – требования к результатам освоения:

Программа ориентирована на достижение следующих целей:

- усвоение знаний по нормативно-правовым основам организации информационной безопасности, изучение стандартов и руководящих документов по защите информационных систем;
- ознакомление с основными угрозами информационной безопасности;
- правилами их выявления, анализа и определение требований к различным уровням обеспечения информационной безопасности;
- формирование научного мировоззрения, навыков индивидуальной самостоятельной работы с учебным материалом.

Содержание каждой темы включает теоретический и практико-ориентированный материал, реализуемый в форме лабораторной работы с использованием средств ИКТ.

Результатом освоения программы учебной дисциплины является овладение обучающимся профессиональными (ПК) и общими (ОК) компетенциями:

Код компетенции	Содержательная часть компетенции
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 1.4	Выполнять тестирование программных модулей.
ПК 1.6	Разрабатывать компоненты проектной и технической документации с использованием графических языков спецификаций
ПК 2.4	Реализовывать методы и технологии защиты информации в базах данных.
ПК 3.2	Выполнять интеграцию модулей в программную систему.

ПК 3.3	Выполнять отладку программного продукта с использованием специализированных программных средств.
ПК 3.4	Осуществлять разработку тестовых наборов и тестовых сценариев.

2. Условия текущей аттестации: аттестация проводится в форме контрольной работы.

Время текущей аттестации:
выполнение 1 ч. 30 мин.

Условия промежуточной аттестации: аттестация проводится в форме экзамена.

Время промежуточной аттестации:
подготовка 40 мин.;
сдача 15 мин.;
всего 55 мин.

3. Программа оценивания контролируемой компетенции:

Текущая аттестация	Контролируемые модули, разделы (темы) дисциплины и их наименование*	Код контролируемой компетенции (или ее части)	Наименование оценочного средства**
№ 1	Раздел № 1. Общие вопросы информационной безопасности Раздел № 2. Государственная система информационной безопасности Раздел № 3. Угрозы безопасности Раздел № 4. Теоретические основы методов защиты информационных систем	ОК 1 – ОК 9, ПК 1.4, ПК 1.6, ПК 2.4, ПК 3.2, ПК 3.3, ПК 3.4	*Комплект КИМ №1*
Промежуточная аттестация		ОК 1 – ОК 9, ПК 1.4, ПК 1.6, ПК 2.4, ПК 3.2, ПК 3.3, ПК 3.4	*Комплект КИМ №2*

Комплект контрольно-измерительного материала №1

УТВЕРЖДАЮ
Заведующий кафедрой _____

_____ _____
подпись, расшифровка подписи

__.__.20__

Специальность 09.02.03 Программирование в компьютерных системах
Дисциплина ОП.09 Информационная безопасность
Форма обучения очное
Вид контроля контрольная работа
Вид аттестации текущая

Контрольная работа (тест)

Задание 1: Меры информационной безопасности направлены на защиту от
- нанесение любого ущерба
- нанесение неприемлемого ущерба
- подглядывание в замочную скважину

Задание 2: Что из перечисленного не относится к числу основных аспектов информационной безопасности:
- доступность
- конфиденциальность
- масштабируемость
- целостность

Задание 3: Затраты организаций на информационную безопасность:
- остаются на одном уровне
- растут
- снижаются

Задание 4: Что из перечисленного относится к числу основных аспектов информационной безопасности:
- конфиденциальность - защита от не санкционированного ознакомления
- приватность - сокрытие информации о личности пользователя
- подотчетность - полнота регистрационной информации о действиях субъектов

Задание 5: Сложность обеспечения информационной безопасности является следствием:
- все большей зависимости общества от информационных систем

- быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним
- невнимания широкой общественности к данной подтеме.

Задание 6: объектно-ориентированный подход помогает справляться с :
- сложностью систем
- недостаточной реактивностью систем
- некачественным пользовательским интерфейсом

Задание 7: контейнеры в компонентных объектных средах предоставляют:
- средства для сохранения компонентов
- механизмы транспортировки компонентов
- общий контекст взаимодействия

Задание 8: Деления на активные и пассивные сущности противоречат:
- стандарту на язык программирования Си
- классической технологии программирования
- основам объектно-ориентированного подхода

Задание 9: Предложим, что при разграничении доступа учитывается семантика программ. В таком случае на игровую программу могут быть наложены следующие ограничения:
- запрет на изменения каких-либо файла, кроме конфигурационных
- запрет на установление сетевых соединений
- запрет на чтение каких-либо файлов, кроме конфигурационных

Задание 10: Необходимость объектно-ориентированного подхода к информационной безопасности является следствием того, что:
- с программно-технической точки зрения, информационная безопасность
– ветвь информационных технологий и должна развиваться по тем же законам
- объектно-ориентированный подход поддержан обширным инструментарием
- объектно-ориентированный подход популярен в академических кругах

Задание 11: В число граней, позволяющих структурировать средства достижения информационной безопасности входят:
- профилактические меры
- мери обеспечения доступности
- законодательные меры

Преподаватель _____ _____

подпись расшифровка подписи

Комплект контрольно-измерительного материала №2

УТВЕРЖДАЮ
Заведующий кафедрой _____

_____ _____
подпись, расшифровка подписи

__.__.20__

Специальность 09.02.03 Программирование в компьютерных системах
Дисциплина ОП.09 Информационная безопасность
Форма обучения очное
Вид контроля экзамен
Вид аттестации промежуточная

Билет №1

1) Основные требования систем защиты информации.
2) Направления обеспечения информационной безопасности (правовая защита).
3) Страховая и лицензионная защита информации.

Преподаватель _____ _____
подпись расшифровка подписи

УТВЕРЖДАЮ
Заведующий кафедрой _____

_____ _____
подпись, расшифровка подписи

__.__.20__

Специальность 09.02.03 Программирование в компьютерных системах
Дисциплина ОП.09 Информационная безопасность
Форма обучения очное
Вид контроля экзамен
Вид аттестации промежуточная

Билет №2

1. Направления обеспечения информационной безопасности (организационная защита).
2. Пресечение разглашения конфиденциальной информации.
3. Противодействие несанкционированному доступу к источникам конфиденциальной информации.

Преподаватель _____ _____
подпись расшифровка подписи