Приложение 1
ОПОП 09.02.07 Информационные системы и программирование

Рабочая программа

Дисциплина **Информационная безопасность**
Базовая подготовка

Иркутск
2024

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.07 Информационные системы и программирование, квалификация специалист по тестированию в области информационных технологий**.**

Программа учебной дисциплины может быть использована в профессиональной подготовке, а также при разработке программ дополнительного профессионального образования специалистов технического профиля.

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина «Информационная безопасность» принадлежит к вариативной части общепрофессионального цикла.

Дисциплина «Информационная безопасность» является общепрофессиональной, устанавливающей базовые знания для усвоения профессиональных компетенций.

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

Целью преподавания дисциплины «Информационная безопасность» является изучение комплекса проблем информационной безопасности организаций различных типов и направлений деятельности; построения, функционирования и совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации; изучение понятий и видов защищаемой информации по законодательству РФ. Изучение данной дисциплины подготавливает студентов к освоению специальных программных средств, связанных с их будущей деятельностью.

Задачи изучения дисциплины включают:

- овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности;
- освоение системных комплексных методов защиты информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения;
- ознакомление с современными законодательными и нормативно-правовыми проблемами обеспечения информационной безопасности;
- приобретение теоретических и практических навыков по основам использования современных методов правовой защиты государственной, коммерческой, служебной, профессиональной и личной тайны, персональных данных в компьютерных системах;

- лицензирования и сертификации в области защиты информации;
- формирование практических навыков и способностей осуществления мероприятий по обеспечению защиты информации с помощью программно-аппаратных средств.

В результате изучения обязательной части учебного цикла обучающийся по общепрофессиональным дисциплинам должен иметь **практический опыт в**:

- обеспечении защиты программного обеспечения компьютерных систем программными средствами;

уметь:

- использовать методы защиты программного обеспечения компьютерных систем;
- анализировать риски и характеристики качества программного обеспечения;
- выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами.

знать:

- основные средства и методы защиты компьютерных систем программными и аппаратными средствами.

Изучение дисциплины способствует освоению **общей компетенции**:

ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

Изучение дисциплины способствует освоению **профессиональной компетенции**, соответствующих основному виду профессиональной деятельности: сопровождение и обслуживание программного обеспечения компьютерных систем:

ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.

1.4. Количество часов на освоение программы учебной дисциплины:

Максимальной учебной нагрузки обучающегося 90 часов, в том числе:

- обязательной аудиторной учебной нагрузки обучающегося 76 часов;
- самостоятельной работы обучающегося 14 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	**90**
Обязательная аудиторная учебная нагрузка (всего)	**76**
в том числе:	
практические занятия	38
Самостоятельная работа обучающегося (всего)	**14**
в том числе:	
внеаудиторная самостоятельная работа	0
в том числе:	
отчеты по выполненным лабораторным работам	14
Итоговая аттестация в форме	***дифференцированного зачета***

2.2. Тематический план и содержание учебной дисциплины 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. Основы информационной безопасности	**Содержание:**	**4**	ОК 1, ПК 4.4
	1. Понятие информационной безопасности. Актуальность информационной безопасности. Принципы обеспечения информационной безопасности. Структура информационной безопасности.		
	2. Система защиты информации. Структура системы защиты информации РФ. Угрозы безопасности в информационной сфере. Комплексный подход к защите информации.		
	Практические занятия:	**4**	
	1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы № 1 «Идентификация источников антропогенных угроз безопасности информации».		
	2. Защита отчета по лабораторной работе № 1. Ответы на контрольные вопросы.		
	Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы, выполнение отчета.	**1**	
Тема 2. Правовая защита информации	**Содержание:**	**4**	ОК 1, ПК 4.4
	1. Структура нормативной базы Российской Федерации по вопросам информационной безопасности. Правовая защита интересов личности, общества и государства от информационных угроз.		
	2. Защита информации по режиму доступа. Классификация информации по видам тайны и степеням конфиденциальности. Защита государственной тайны. Защита коммерческой тайны. Защита персональных данных.		
	Практические занятия:	**4**	
	1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы №2 «Разработка частной модели угроз организации».		
	2. Защита отчета по лабораторной работе № 2. Ответы на контрольные вопросы.		
	Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы, выполнение отчета.	**1**	
Тема 3. Организационная защита информации	**Содержание:**	**4**	ОК 1, ПК 4.4
	1. Зоны ответственности. Локальные нормативные акты в области информационной безопасности. Административный уровень организационной защиты информации. Оценка рисков		

	информационной безопасности. Политика информационной безопасности.		
	2. Процедурный уровень организационной защиты информации. Организация службы безопасности предприятия. Организация конфиденциального документооборота. Грифы ограничения доступа к документам.		
	Практические занятия:	**4**	
	1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы №3 «Политика информационной безопасности».		
	2. Защита отчета по лабораторной работе № 3. Ответы на контрольные вопросы.		
	Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы, выполнение отчета.	**1**	
Тема 4. Защита информации в компьютерных системах	**Содержание:**	**8**	ОК 1, ПК 4.4
	1. Анализ угроз информационной безопасности компьютерных систем. Технологии защиты информации в компьютерных системах.		
	2. Идентификация, аутентификация и управление доступом. Обеспечение безопасности операционных систем.		
	3. Безопасность межсетевого обмена данными. Технологии межсетевого экранирования. Технологии виртуальных защищенных сетей (VPN).		
	4. Анализ защищенности и обнаружение атак. Технологии резервного копирования и восстановления данных.		
	Практические занятия:	**8**	
	1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы №4 «Настройка политики управления доступом».		
	2. Защита отчета по лабораторной работе № 4. Ответы на контрольные вопросы.		
	3. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы №5 «Применение электронной подписи».		
	4. Защита отчета по лабораторной работе № 5. Ответы на контрольные вопросы.		
	Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы, выполнение отчета.	**1**	
Тема 5. Методы криптографического преобразования информации	**Содержание:**	**4**	ОК 1, ПК 4.4
	1. Классификация методов криптографического закрытия информации. Симметричные криптосистемы. Криптосистемы с открытым ключом.		
	2. Практическое применение криптографии. Квантовая криптография. Стеганография. Элек-		

	тронная подпись.		
	Практические занятия:	**4**	
	1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы № 6 «Шифрованная файловая система Windows».		
	2. Защита отчета по лабораторной работе № 6. Ответы на контрольные вопросы.		
	Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы.	**1**	
Тема 6. Вредоносное программное обеспечение	**Содержание:**	**4**	ОК 1, ПК 4.4
	1. Условия существования вредоносных программ. Классификация вредоносных программ. Эволюция компьютерных вирусов.		
	2. Защита компьютерных систем от воздействия вредоносных программ. Основы работы антивирусных программ. Защита от СПАМА.		
	Практические занятия:	**4**	
	1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы № 7 «Защита информации в файлах данных средствами MS Office».		
	2. Защита отчета по лабораторной работе № 7. Ответы на контрольные вопросы.		
	Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы, выполнение отчета.	**1**	
Тема 7. Инженерно-техническая защита информации	**Содержание:**	**6**	ОК 1, ПК 4.4
	1. Технические каналы утечки информации. Средства выявления каналов утечки информации.		
	2. Методы и способы защиты информации от утечки по техническим каналам.		
	3. Физическая укрепленность объекта информатизации.		
	Практические занятия:	**4**	
	1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы № 8 «Профилактика проникновения вредоносного программного обеспечения».		
	2. Защита отчета по лабораторной работе № 8. Ответы на контрольные вопросы.		
	Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы.	**1**	
Тема 8. Управление информационной безопасностью	**Содержание:**	**4**	ОК 1, ПК 4.4
	1. Ответственность, за правонарушения в области информационной безопасности. Лицензирование, сертификация и аттестация в сфере защиты информации. Комплексный подход к		

	защите информации.		
	2. Стандарты и спецификации в области информационной безопасности. Анализ защищенности информационной системы. Управление информационной безопасностью. Практические правила управления информационной безопасностью.		
	Практические занятия:	**6**	
	1. Устный опрос по теоретическому материалу для получения допуска к выполнению лабораторной работы. Выполнение лабораторной работы № 9 «Обеспечение безопасности объекта информатизации».		
	2. Защита отчета по лабораторной работе № 9. Ответы на контрольные вопросы.		
	3. Итоговый тест.		
	Самостоятельная работа обучающихся: изучение теоретического материала для подготовки к выполнению лабораторной работы и ответов на контрольные вопросы, выполнение отчета.	**1**	
	Всего:	**76**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Лаборатория «Программного обеспечения и сопровождения компьютерных систем» оснащенная необходимым для реализации программы учебной дисциплины оборудованием:

- автоматизированные рабочие места на 12-15 обучающихся (процессор не ниже Core i3, оперативная память объемом не менее 4 Гб) или аналоги;
- автоматизированное рабочее место преподавателя (процессор не ниже Core i3, оперативная память объемом не менее 4 Гб) или аналоги;
- проектор и экран;
- маркерная доска;

Программное обеспечение общего и профессионального назначения

3.2. Информационное обеспечение обучения

Основные источники:

1. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87995.html (дата обращения: 07.06.2024). — Режим доступа: для авторизир. пользователей.
2. Технологии защиты информации в компьютерных сетях : учебное пособие для СПО / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — Саратов : Профобразование, 2021. — 368 с. — ISBN 978-5-4488-1014-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102207.html (дата обращения: 07.06.2024). — Режим доступа: для авторизир. пользователей.
3. Фомин, Д. В. Информационная безопасность : учебник / Д. В. Фомин. — Москва : Ай Пи Ар Медиа, 2022. — 222 с. — ISBN 978-5-4497-1548-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/118876.html (дата обращения: 07.06.2024). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/118876.
4. Бусько М.М. Информационная безопасность и защита информации : учеб. пособие.- Иркутск: Изд-во БГУ, 2022.- 220 с.

Дополнительные источники:

1. Галатенко В.А. Основы информационной безопасности : учебное пособие / Галатенко В.А.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс

IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/97562.html (дата обращения: 07.06.2024). — Режим доступа: для авторизир. пользователей.
2. Информационная безопасность. Практические аспекты : учебник для вузов / Л. Х. Сафиуллина, А. Р. Касимова, Я. С. Рябов [и др.]. — Санкт-Петербург : Интермедия, 2021. — 240 с. — ISBN 978-5-4383-0205-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/103997.html (дата обращения: 07.06.2024). — Режим доступа: для авторизир. пользователей.
3. Банк данных угроз безопасности информации. Федеральная служба по техническому и экспортному контролю. Государственный научно-исследовательский испытательный институт проблем технической защиты информации. http://bdu.fstec.ru/ (07.06.2024)
4. Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00. http://fstec.ru/component/attachments/download/489

Интернет-ресурсы

1. https://fstec.ru/ — Федеральная служба по техническому и экспортному контролю. Нормативная база.
2. http://window.edu.ru/ — Единое окно доступа к образовательным ресурсам.
3. http://citforum.ru/ — Сервер Информационных Технологий.
4. http://fcior.edu.ru/ — Федеральный центр электронных образовательных ресурсов.
5. http://www.intuit.ru/ — Национальный Открытый Университет.
6. http://www.ixbt.com — специализированный российский информационно-аналитический сайт с самыми актуальными новостями из сферы IT.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе выполнения лабораторных работ, тестирования, а также ответов на контрольные вопросы.

Результаты обучения	***Критерии оценки***	***Формы и методы оценки***
Перечень знаний, осваиваемых в рамках дисциплины: - Основные средства и методы защиты компьютерных систем программными и аппаратными средствами. *Перечень умений, осваиваемых в рамках дисциплины:* - Использовать методы защиты программного обеспечения компьютерных систем. - Анализировать риски и характеристики качества программного обеспечения. - Выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами.	«Отлично» — теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» — теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» — теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» — теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Текущий контроль в форме: – наблюдения за выполнением практического задания. (деятельностью студента); – защиты отчетов по лабораторным работам; – оценки выполнения практического задания(работы); – устных опросов; – компьютерного тестирования на знание терминологии по теме. Зачет по дисциплине.