

Государственное бюджетное профессиональное образовательное учреждение
«Южно-Уральский государственный колледж»

УТВЕРЖДАЮ
Зам. директора по учебной работе
_____ Т.С. Занова
«25» августа 2020 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.13 Информационная безопасность

по специальности среднего
профессионального образования
09.02.07 Информационные системы и программирование

Квалификация: Программист

Рабочая программа учебной дисциплины разработана на основе примерной программы по специальности СПО 09.02.07 Информационные системы и программирование укрупнённой группы специальностей 09.00.00 **Информатика и вычислительная техника**

Рекомендована Государственным бюджетным профессиональным образовательным учреждением «Южно-Уральский государственный колледж».

Организация-разработчик рабочей программы: Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный колледж».

Разработчики:

Назарова Наталья Александровна, преподаватель

Рассмотрена и одобрена на заседании ПЦК «Информационных технологий»
Протокол № 11 от «20» июня 2020 г.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	стр. 4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	5
3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	11
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	13
5. ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ПРОГРАММЫ В ДРУГИХ РАБОЧИХ ОСНОВНЫХ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММАХ (РООП)	24

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

1.1 Область применения рабочей программы

Рабочая программа учебной дисциплины является частью рабочей основной образовательной программы в соответствии с ФГОС СПО 09.02.07 Информационные системы и программирование.

1.2 Место дисциплины в структуре программы подготовки специалистов среднего звена:

дисциплина принадлежит к общепрофессиональному циклу.

1.3 Цель и планируемые результаты освоения дисциплины:

В результате освоения дисциплины обучающийся должен уметь:

- применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности;
- выявлять основные угрозы информационной безопасности;
- производить установку и настройку типовых программных средств защиты информации;
- обеспечивать антивирусную защиту;
- фильтровать сетевые пакеты межсетевым экраном;
- использовать типовые криптографические средства и методы защиты информации, в том числе электронную цифровую подпись;
- выполнять операции резервного копирования и восстановления данных.

В результате освоения дисциплины обучающийся должен знать:

- сущность и понятие информационной безопасности, характеристику её составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды угроз информационной безопасности;
- основные положения комплексного подхода к защите информации;
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ и ФСТЭК РФ в данной области;
- принципы архитектурной безопасности;
- современные программно-технические средства обеспечения информационной безопасности;
- виды систем идентификации и аутентификации;
- типовые модели управления доступом;
- типовые средства и методы ведения аудита;
- основные понятия криптографии;
- типовые криптографические алгоритмы, применяемые для защиты информации;

- типовые методы скрытия информации;
- методы резервного копирования данных.

В результате освоения дисциплины обучающийся осваивает **элементы компетенций**:

Общие компетенции	Дескрипторы сформированности (действия)	Уметь	Знать
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам,	правильно распознает задачу в профессиональном контексте точно перечисляет методы работы в сфере ИТ правильно выполняет этапы по решению задачи точно называет структуру плана для решения задачи правильно осуществляет поиск информации точно называет порядок оценки результатов решения задачи правильно составляет план действий правильно определяет ресурсы для решения задачи правильно применяет методы работы в сфере ИТ точно и правильно может реализовать составленный план по решению задачи объективно оценивает результат своих действий	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	правильно определяет задачи и ищет информацию средствами ИТ точно и правильно перечисляет номенклатуру информационных источников правильно перечисляет приемы структурирования информации точно и правильно планирует процесс поиска информации и ее структурирование средствами ИТ	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации

Общие компетенции	Дескрипторы сформированности (действия)	Уметь	Знать
	правильно определяет формат оформления поиска результатов	поиска	
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.	точно и правильно определяет актуальность нормативно-правовой документации средствами ИТ правильно применяет современную научную и профессиональную терминологию правильно называет возможные траектории профессионального развития и самообразования в сфере ИТ	Определять актуальность нормативно-правовой документации в профессиональной деятельности.	Содержание актуальной нормативно-правовой документации. Современная научная и профессиональная терминология. Возможные траектории профессионального развития и самообразования
ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	правильно организывает работу коллектива правильно взаимодействует с коллегами в ходе работы на занятиях	организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности	психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	правильно оформляет документы с использованием ИТ точно называет правила оформления документов средствами ИТ	грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе	особенности социального и культурного контекста; правила оформления документов и построения устных сообщений
ОК 9. Использовать информационные технологии в профессиональной деятельности	правильно применяет средства информационных технологий для решения профессиональных задач правильно определяет современные средства и устройства информатизации правильно и точно использует современное программное обеспечение точно называет порядок применения ПО в сфере ИТ	применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение	современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках	правильно понимает тексты на темы, связанные со сферой ИТ правильно применяет	понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и	правила построения простых и сложных предложений на профессиональные темы; основные

Общие компетенции	Дескрипторы сформированности (действия)	Уметь	Знать
	диалоги на темы, связанные со сферой ИТ точно и правильно строит простые высказывания о себе и о сфере ИТ правильно объясняет свои действия правильно пишет и читает тексты ИТ-направленности	бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы	общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности

Профессиональные компетенции	Дескрипторы сформированности (действия)	Уметь	Знать
ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами	Называет основные средства и методы защиты компьютерных систем программными и аппаратными средствами Правильно делает выбор методов защиты программного обеспечения компьютерных систем.	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.	Основные средства и методы защиты компьютерных систем программными и аппаратными средствами.
ПК 11.6. Защищать информацию в базе данных с использованием технологии защиты информации	обосновывает период резервного копирования БД на основе анализа обращений пользователей; выполняет резервное копирование БД; выполняет восстановление состояния БД на заданную дату.	Выполнять установку и настройку программного обеспечения для обеспечения работы пользователя с базой данных. Обеспечивать информационную безопасность на уровне базы данных.	Методы организации целостности данных. Способы контроля доступа к данным и управления привилегиями. Основы разработки приложений баз данных. Основные методы и средства защиты данных в базе данных

1.4 Количество часов на освоение программы учебной дисциплины:

Объем образовательной нагрузки обучающегося – 92 часа,

Из них нагрузки дисциплины во взаимодействии с преподавателем - 92 часа,
в том числе:
теоретического обучения – 46 часов,
практической подготовки – 72 часа,
лабораторно-практических работ – 46 часов;
курсового проектирования – 0 часов,
экзамены и консультации – 0 часов;
самостоятельной учебной работы обучающегося – 0 часов.

2 СТРУКТУРА СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Общий объем образовательной нагрузки обучающегося	92
Самостоятельная учебная работа обучающегося	-
Нагрузка дисциплины во взаимодействии с преподавателем	92
в том числе:	
теоретическое обучение	46
практическая подготовка	72
лабораторные занятия (если предусмотрено)	-
практические занятия (если предусмотрено)	46
курсовая работа (проект) (если предусмотрено)	-
контрольная работа	-
<i>Самостоятельная работа</i>	0
Промежуточная аттестация проводится в форме дифференцированного зачёта	

2.2. Тематический план и содержание учебной дисциплины Информационная безопасность

<i>Наименование разделов и тем</i>	<i>Содержание учебного материала и формы организации деятельности обучающихся</i>	<i>Уровень освоения</i>	<i>Объем часов</i>	<i>Осваиваемые элементы компетенций</i>
<i>1</i>	<i>2</i>		<i>3</i>	<i>4</i>
Тема 1. Понятие и основные составляющие ИБ	Содержание учебного материала	Уровень освоения		ОК 1, ОК 2, ОК 4, ОК 5, ОК 9, ОК 10, ПК4.4
	1. Сущность и понятие ИБ. Междисциплинарные связи ИБ с базами данных, системным и прикладным программированием, компьютерными сетями, правоведением. Внутренняя информация. Внешняя информация. Свойства информации. Необходимость и цели защиты информации. Определение ИБ. Проблема ИБ. Место ИБ в системе национальной безопасности страны. Составляющие ИБ.	1	2	
	Тематика практических занятий и лабораторных работ 1. Анализ примеров нарушений ИБ. Выявление значимых составляющих ИБ и характеристик ИС в конкретных ситуациях	2	2	
	Практическая подготовка		-	
	Самостоятельная работа обучающихся		-	
Тема 2. Виды угроз ИБ	Содержание учебного материала	Уровень освоения		ОК 1, ОК 2, ОК 4, ОК 5, ОК 9, ОК 10, ПК4.4
	1. Понятие угрозы. Угроза ИБ. Уязвимость. Окно опасности. Критерии классификации угроз. 2. Угрозы нарушения конфиденциальности. Несанкционированный доступ к информации. Перехват данных. Кража носителей информации. Методы социальной инженерии. Фишинг. Инсайдеры. Злоупотребление полномочиями 3. Угрозы нарушения целостности. Статическая целостность. Динамическая целостность. Нарушения аутентичности. Нарушения апеллируемости. Подлог (фарминг). SQL-инъекция. Нарушение атомарности транзакций. Активное прослушивание. Атака «человек посередине». Непреднамеренные ошибки.	1	8	

<i>Наименование разделов и тем</i>	<i>Содержание учебного материала и формы организации деятельности обучающихся</i>	<i>Уровень освоения</i>	<i>Объем часов</i>	<i>Осваиваемые элементы компетенций</i>
<i>1</i>	<i>2</i>		<i>3</i>	<i>4</i>
	4. Угрозы нарушения доступности. Отказ пользователей. Внутренний отказ ИС. Отказ поддерживающей инфраструктуры. Агрессивное потребление ресурсов. Атаки на отказ в обслуживании. Переполнение буфера.			
	Тематика практических занятий 1. Решение ситуационных задач: выявление угроз ИБ в конкретных ситуациях. Демонстрация подлога при разрешении символического имени в IP-адрес путём модификации файла hosts. Изложение схемы атаки на отказ в обслуживании (атаки SYN-шторм, ICMP-шторм).	2	2	
	Практическая подготовка		8	
	Самостоятельная работа обучающихся		-	
Тема 3. Вредоносное программное обеспечение (ПО)	Содержание учебного материала	Уровень освоения	6	ОК 1, ОК 2, ОК 4, ОК 5, ОК 9, ОК 10, ПК4.4
	1. Понятие вредоносного ПО и каналы его распространения. Вредоносная программа. Логическая бомба. Основные каналы распространения: локальная вычислительная сеть; сеть Интернет; электронная почта; мобильные носители. Методы защиты от вредоносного ПО. Классификация вредоносного ПО. Компьютерный вирус. Жизненный цикл компьютерного вируса. Классификация компьютерных вирусов. Тестовый вирус Eicar. Сетевой червь. Жизненный цикл сетевого червя. Классификация сетевых червей. 2. Классификация вредоносного ПО. Троянская программа. Жизненный цикл троянской программы. Классификация троянских программ. Условно-опасное ПО. Эксплойт. Руткит. Шпионское ПО. Компьютер-зомби. Ботнет. 3. Признаки заражения компьютера вредоносным ПО. Принципы работы антивирусного ПО. Явные проявления: всплывающие сообщения; изменение настроек	1		

<i>Наименование разделов и тем</i>	<i>Содержание учебного материала и формы организации деятельности обучающихся</i>	<i>Уровень освоения</i>	<i>Объем часов</i>	<i>Осваиваемые элементы компетенций</i>
<i>1</i>	<i>2</i>		<i>3</i>	<i>4</i>
	браузера; несанкционированный выход в Интернет. Косвенные проявления: сбои в работе операционной системы и ПО; блокирование антивирусного ПО и сайтов; несанкционированная рассылка электронных писем. Скрытые проявления: наличие подозрительных файлов и процессов; подозрительная сетевая активность.. Резидентная проверка. Сканирование по требованию. Сигнатурный анализ. Эвристический анализ. Проактивная защита. Антивирусное ядро. Карантин. Механизм безопасного исполнения программного кода («песочница»).			
	Тематика практических занятий и лабораторных работ 1. Определение функциональных возможностей и принципов работы троянской программы на примере клавиатурного шпиона. 2. Выполнение проверки компьютера на наличие признаков заражения вредоносным ПО: исследование настроек браузера, запущенных процессов, элементов автозапуска, сетевой активности. 3. Обоснование применения норм уголовного права в конкретных ситуациях, связанных с созданием и использованием вредоносного ПО. 4. Выполнение установки антивирусного ПО. Обоснование выбора устанавливаемых компонентов. Обновление антивирусных баз. Выполнение настройки параметров антивирусной и проактивной защиты. Настройка уведомлений. Выполнение антивирусного сканирования с заданными параметрами	2	8	
	Практическая подготовка		12	
	Самостоятельная работа обучающихся		-	
Тема 4. Правовые основы обеспечения	Содержание учебного материала	Уровень освоения	4	ОК 1, ОК 2, ОК 4, ОК 5,

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Уровень освоения	Объем часов	Осваиваемые элементы компетенций
1	2		3	4
ИБ	<p>1. Структура правового обеспечения ИБ. Международные конвенции и федеральные законы РФ. Указы Президента РФ. Постановления Правительства РФ. Государственные стандарты. Руководящие документы ФСТЭК (Гостехкомиссии) и ФСБ РФ. Локальные нормативные акты и методические рекомендации.</p> <p>2. Классификация информации по видам тайн. Защита прав собственности на информацию. Уровни доступа к информации. Государственная тайна и степени её секретности (грифы). Коммерческая тайна и градации её ценности. Банковская тайна. Виды профессиональных тайн. Виды служебных тайн. Объекты интеллектуальной собственности. Права владения, пользования и распоряжения информацией. Защита авторских прав в ГК РФ. Персональные данные</p>	1		ОК 9, ОК 10,
	<p>Тематика практических занятий и лабораторных работ</p> <p>1. Решение ситуационных задач: нахождение применимых правовых норм в заданных условиях.</p>	2	2	
	Практическая подготовка		6	
	Самостоятельная работа обучающихся		-	
Тема 5. Оценочные стандарты и технические спецификации в области ИБ	Содержание учебного материала	Уровень освоения	6	ОК 1, ОК 2, ОК 4, ОК 5, ОК 9, ОК 10,
	<p>1. «Оранжевая книга». ИБ распределённых систем. Рекомендации X.800. Безопасная система. Доверенная система. Периметр безопасности. Основные механизмы безопасности. Классификация ИС по степени доверия безопасности. Сетевые функции безопасности. Сетевые механизмы безопасности. Взаимосвязь функций и механизмов. Обязанности администратора безопасности.</p> <p>2. «Общие критерии». Стандарт ISO/IEC 15408. Управление ИБ. Серия стандартов ISO/IEC 27000. Среда безопасности и её аспекты. Цели безопасности.</p>	1		

<i>Наименование разделов и тем</i>	<i>Содержание учебного материала и формы организации деятельности обучающихся</i>	<i>Уровень освоения</i>	<i>Объем часов</i>	<i>Осваиваемые элементы компетенций</i>
<i>1</i>	<i>2</i>		<i>3</i>	<i>4</i>
	<p>Функциональные требования безопасности. Требования доверия. Профиль защиты. Задание по безопасности. ГОСТ Р 15408-2002. Система управления информационной безопасностью. Модель PDCA (цикл Деминга). Мероприятия по управлению ИБ (сервисы безопасности). ГОСТ Р 17799-2005.</p> <p>3. Руководящие документы ФСТЭК (Гостехкомиссии) и ФСБ. Спецификации RFC Роль ФСТЭК и ФСБ в обеспечении ИБ. Обзор руководящих документов ФСТЭК. Классификация автоматизированных систем по уровню защищённости от несанкционированного доступа. Требования к защищённости автоматизированных систем. Нормативные документы ФСТЭК и ФСБ по организации защиты персональных данных (ПДн). Понятие RFC. Жизненный цикл и виды RFC. RFC 1244, 2196 «Руководство по информационной безопасности предприятия». RFC 2350 «Как реагировать на нарушения информационной безопасности»</p>			
	<p>Тематика практических занятий и лабораторных работ</p> <p>1. Изложение практических рекомендаций по управлению ИБ по отношению к одному из сервисов безопасности, описанных в ГОСТ Р 17799-2005.</p> <p>2. Определение класса ИС персональных данных (ИСПДн) для ИС гипотетической организации в соответствии с совместным приказом ФСТЭК, ФСБ и Мининформсвязи РФ № 55/86/20 от 13 февраля 2008 г.</p> <p>3. Выполнение оценки исходной степени защищённости ИСПДн, выделение актуальных угроз безопасности в соответствии с «Методикой определения актуальных угроз безопасности ПДн при их обработке в ИСПДн».</p>	2	6	
	Практическая подготовка		6	
	Самостоятельная работа обучающихся		-	

<i>Наименование разделов и тем</i>	<i>Содержание учебного материала и формы организации деятельности обучающихся</i>	<i>Уровень освоения</i>	<i>Объем часов</i>	<i>Осваиваемые элементы компетенций</i>
<i>1</i>	<i>2</i>		<i>3</i>	<i>4</i>
Тема 6. Принципы обеспечения ИБ на программно-техническом уровне	Содержание учебного материала	Уровень освоения	4	ОК 1, ОК 2, ОК 4, ОК 5, ОК 9, ОК 10,
	1. Административный уровень ИБ. Процедурный уровень ИБ. Политика безопасности. Уровни политики безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом ИС. Управление рисками. Этапы управления рисками. Вопросы безопасности, связанные с персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушение режима безопасности. Планирование восстановительных работ.	1		
	2. Основные понятия программно-технического уровня ИБ. Принципы архитектурной безопасности. Сервисы безопасности программно-технического уровня. Место сервисов безопасности в архитектуре ИС. Виды мер безопасности. Особенности современных ИС, существенные с точки зрения ИБ. Непрерывность защиты. Следование стандартам. Иерархическая организация ИС. Усиление самого слабого звена. Невозможность перехода в небезопасное состояние. Минимизация привилегий. Разделение обязанностей. Эшелонированность обороны. Разнообразие защитных средств. Простота и управляемость ИС. Минимизация защитных средств на клиентских системах			
	Тематика практических занятий и лабораторных работ	2	2	
	1. Решение ситуационных задач: обоснование применения принципов архитектурной безопасности в заданных условиях		4	
	Практическая подготовка		4	
	Самостоятельная работа обучающихся		-	
Тема 7. Средства обеспечения	Содержание учебного материала	Уровень освоения	8	ОК 1, ОК 2, ОК 4, ОК 5,

<i>Наименование разделов и тем</i>	<i>Содержание учебного материала и формы организации деятельности обучающихся</i>	<i>Уровень освоения</i>	<i>Объем часов</i>	<i>Осваиваемые элементы компетенций</i>
<i>1</i>	<i>2</i>		<i>3</i>	<i>4</i>
конфиденциальности	<p>1. Построение систем защиты от угроз нарушения конфиденциальности. Идентификация и аутентификация. Структура системы защиты от угроз нарушения конфиденциальности. Организационные меры защиты. Базовая схема идентификации и аутентификации. Виды аутентификации. Виды аутентификаторов. Виды систем идентификации и аутентификации. Особенности парольных систем аутентификации. Методы хранения паролей. Идентификатор безопасности. Сервер аутентификации Kerberos. Особенности биометрических систем идентификации и аутентификации.</p> <p>2. Управление доступом. Протоколирование и аудит. Матрица доступа. Модели управления доступом. Дискреционное и мандатное управление доступом. Списки контроля доступа (ACL). Ролевое управление доступом. Цели протоколирования и аудита. События, подлежащие аудиту. Информация, подлежащая регистрации. Типовые средства и методы ведения аудита. Системные списки контроля доступа (SACL). Выборочное протоколирование. Аудит успехов и аудит отказов. Активный аудит. Сигнатура атаки. Системы обнаружения вторжений. Системы предотвращения вторжений.</p> <p>3. Симметричное и асимметричное шифрование. Скрытие информации (стеганография). Криптография. Криптоанализ. Криптосистема. Криптографический ключ. Криптографическая стойкость. Структура симметричной и асимметричной криптосистемы. Открытый и закрытый ключи. Сферы использования симметричной и асимметричной криптосистемы. Типовые криптографические алгоритмы. Криптографический алгоритм RSA. Составные ключи. Инфраструктура открытых ключей. Цифровой сертификат. Удостоверяющий центр. Назначение стеганографии.</p>	<i>1</i>		ОК 9, ОК 10,

<i>Наименование разделов и тем</i>	<i>Содержание учебного материала и формы организации деятельности обучающихся</i>	<i>Уровень освоения</i>	<i>Объем часов</i>	<i>Осваиваемые элементы компетенций</i>
<i>1</i>	<i>2</i>		<i>3</i>	<i>4</i>
	<p>Классификация методов стеганографического преобразования. Типы стеганографических алгоритмов. Алгоритм LSA. Особенности применения стеганографии.</p> <p>4. Экранирование и анализ защищённости. Туннелирование. Назначение экранирования. Межсетевой экран. Архитектурные аспекты экранирования. Пакетный фильтр. Шлюз сеансового уровня. Шлюз прикладного уровня. Прокси-сервер. Системы анализа защищённости. Цели туннелирования. Виртуальные частные сети.</p>			
	<p>Тематика практических занятий и лабораторных работ</p> <ol style="list-style-type: none"> 1. Создание пользователей и групп в операционной системе (ОС) Windows. Решение задач поиска и сброса паролей пользователей. 2. Выполнение настройки системы парольной защиты в локальной политике безопасности ОС Windows. 3. Создание списков контроля доступа и назначение прав доступа на уровне файловой системы NTFS в заданных условиях. 4. Выполнение настройки параметров аудита в ОС Windows в заданных условиях. Получение и интерпретация результатов аудита. 5. Выполнение установки ПО для работы с инфраструктурой открытых ключей. Создание открытого и закрытого криптографических ключей. 6. Выполнение установки ПО для стеганографического преобразования. Выполнение операций по скрытию и обмену скрытой информацией. 7. Выполнение установки сетевого сканера. Определение списка открытых портов в ОС Windows при помощи сетевого сканера. 8. Выполнение настройки межсетевого экрана: создание правил фильтрации пакетов для предотвращения доступа к 	<i>2</i>	<i>18</i>	

<i>Наименование разделов и тем</i>	<i>Содержание учебного материала и формы организации деятельности обучающихся</i>	<i>Уровень освоения</i>	<i>Объем часов</i>	<i>Осваиваемые элементы компетенций</i>
<i>1</i>	<i>2</i>		<i>3</i>	<i>4</i>
	внутренним сервисам. 9. Выполнение настройки межсетевого экрана: создание правил фильтрации пакетов для предотвращения доступа к внутренним сервисам.			
	<i>Практическая подготовка</i>		26	
	<i>Самостоятельная работа обучающихся</i>		-	
Тема 8. Средства обеспечения целостности	<i>Содержание учебного материала</i>	<i>Уровень освоения</i>	4	ОК 1, ОК 2, ОК 4, ОК 5, ОК 9, ОК 10, ПК4.4
	1. Построение систем защиты от угроз нарушения целостности. Принципы обеспечения целостности. Структура системы защиты от угроз нарушения целостности. 2. Криптографические хеш-функции. Электронная цифровая подпись (ЭЦП). Назначение хеш-функций. Коллизия. Причины возникновения коллизий. Виды хеш-функций. Соль (модификатор ключа). Назначение и применение ЭЦП. Симметричная и асимметричная схема ЭЦП. Реализация механизма ЭЦП. Формирование ЭЦП. Проверка ЭЦП. Модели атак. Коллизии первого и второго рода.	1		
	<i>Тематика практических занятий и лабораторных работ</i>	2	4	
	1. Установка ПО для расчёта хешей. Определение целостности файла при помощи хеш-функций MD5 и SHA-1. 2. Выполнение операций по обмену открытыми ключами через инфраструктуру открытых ключей, отправке и получению зашифрованных и подписанных ЭЦП документов.		8	
	<i>Практическая подготовка</i>		-	
	<i>Самостоятельная работа обучающихся</i>		-	
Тема 9. Средства обеспечения	<i>Содержание учебного материала</i>	<i>Уровень освоения</i>	4	ОК 1, ОК 2, ОК 4, ОК 5,

<i>Наименование разделов и тем</i>	<i>Содержание учебного материала и формы организации деятельности обучающихся</i>	<i>Уровень освоения</i>	<i>Объем часов</i>	<i>Осваиваемые элементы компетенций</i>
<i>1</i>	<i>2</i>		<i>3</i>	<i>4</i>
доступности	1. Задача обеспечения высокой доступности. Построение систем защиты от угроз нарушения доступности. Интенсивность отказов. Среднее время наработки на отказ. Виды мер обеспечения высокой доступности. Качество обслуживания (QoS). Структура системы защиты от угроз нарушения доступности. Дублирование каналов связи и сетевого оборудования. Дублирование серверов. Отказоустойчивый кластер. Резервное копирование данных. Методы резервного копирования данных. RAID-массивы. Обеспечение обслуживаемости. 2. Управление информационными сервисами и сервисами безопасности. Состав управления. Функциональные области управления. Архитектура «менеджер—агент». Доверенное управление. Упреждающее управление. Системы управления. Контроль производительности.	<i>1</i>		ОК 9, ОК 10, ПК4.4
	Тематика практических занятий и лабораторных работ 1. Выполнение настройки параметров резервного копирования дисков в соответствии с разработанным планом. Выполнение резервного копирования и восстановления данных. Создание программного RAID-массива типа «зеркало». Выполнение замеров производительности и тестирование отказа одного из элементов RAID-массива	<i>2</i>	2	
	Практическая подготовка		6	
	Самостоятельная работа обучающихся		-	
	ИТОГО		92	

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ 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».

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемых для использования в образовательном процессе

3.2.1. Печатные издания

1. **Баранова, Е. К.** Основы информационной безопасности: учебник / Е. К. Баранова, А. В. Бабаш. - Москва: РИОР: ИНФРА-М, 2021. — 202 с.

2. **Партыка, Т. Л.** Информационная безопасность: учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2021. — 432 с.

3. **Родичев, Ю.А.** Нормативная база и стандарты в области информационной безопасности. Учебное пособие / Ю.А. Родичев. - Санкт-Петербург: Питер, 2021. - 256 с.

4. **Сычев, Ю. Н.** Защита информации и информационная безопасность: учебное пособие / Ю.Н. Сычев. — Москва: ИНФРА-М, 2021. — 201 с.

5. **Сычев, Ю. Н.** Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие / Ю.Н. Сычев. — Москва: ИНФРА-М, 2021. — 223 с.

Электронные ресурсы:

1. Портал для профессионалов информационной безопасности: сайт. — Москва. — Обновляется в течение суток. —URL:<http://www.itsec.ru/> (дата обращения 10. 06.2021). — Текст: электронный

2. Информационный портал по информационной безопасности: сайт. — Москва. — Обновляется в течение суток. —URL: <https://www.securitylab.ru/> (дата обращения 10. 06.2021). — Текст: электронный

3. Новости информационной безопасности: сайт. — Москва. — Обновляется в течение суток. —URL: <https://www.anti-malware.ru/news> (дата обращения 10. 06.2021). — Текст: электронный

4. Компьютерная справочная правовая система в России: сайт. — Москва. —URL: <http://www.consultant.ru/> (дата обращения 10. 06.2021). — Текст: электронный

3.3. Организация образовательного процесса

Занятия по изучению данной дисциплины проводится в традиционной форме обучения, которая характеризуется традиционной подачей материала при непосредственном общении обучаемых с преподавателем и возможностью диалога между ними, а также проведением практических занятий. При этом рекомендуется использование ИКТ и других технических средств обучения. Каждый обучающийся должен иметь доступ к компьютеру на все время обучения, оборудование должно быть соответствующим.

Для демонстрации материала на лекционных занятиях необходим мультимедийный проектор.

Входные требования к обучающимся: особых требований нет.

3.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров:

Реализация образовательной программы обеспечивается руководящими и педагогическими работниками образовательной организации, а также лицами, привлекаемыми к реализации образовательной программы на условиях гражданско-правового договора, в том числе из числа руководителей и работников организаций, деятельность которых связана с направленностью реализуемой образовательной программы (имеющих стаж работы в данной профессиональной области не менее 3 лет).

Квалификация педагогических работников образовательной организации должна отвечать квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональных стандартах (при наличии).

Педагогические работники получают дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в организациях, направление деятельности которых соответствует области профессиональной деятельности, указанной в пункте 1.5 ФГОС СПО по данной специальности, не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.

Доля педагогических работников (в приведенных к целочисленным значениям ставок), обеспечивающих освоение обучающимися профессиональных модулей, имеющих опыт деятельности не менее 3 лет в организациях, направление деятельности которых соответствует области профессиональной деятельности, указанной в пункте 1.5 ФГОС СПО данной специальности, в общем числе педагогических работников, реализующих образовательную программу, должна быть не менее 25 %.

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

<i>Результаты обучения</i>	<i>Критерии оценки</i>	<i>Формы и методы оценки</i>
<p><i>Перечень умений, осваиваемых в рамках дисциплины:</i></p> <ul style="list-style-type: none"> – применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности; – выявлять основные угрозы информационной безопасности; – производить установку и настройку типовых программных средств защиты информации; – обеспечивать антивирусную защиту; – фильтровать сетевые пакеты межсетевым экраном; – использовать типовые криптографические средства и методы защиты информации, в том числе электронную цифровую подпись; – выполнять операции резервного копирования и восстановления данных. 	<p>«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко.</p> <p>«Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками.</p>	<ul style="list-style-type: none"> • Компьютерное тестирование на знание терминологии по теме; • Наблюдение за выполнением практического задания. (деятельностью студента) • Оценка выполнения практического задания(работы)

<p><i>Перечень знаний, осваиваемых в рамках дисциплины:</i></p> <ul style="list-style-type: none"> – сущность и понятие информационной безопасности, характеристику её составляющих; – место информационной безопасности в системе национальной безопасности страны; – виды угроз информационной безопасности; – основные положения комплексного подхода к защите информации; – основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ и ФСТЭК РФ в данной области; – принципы архитектурной безопасности; – современные программно-технические средства обеспечения информационной безопасности; – виды систем идентификации и аутентификации; – типовые модели управления доступом; – типовые средства и методы ведения аудита; – основные понятия криптографии; – типовые криптографические алгоритмы, применяемые для защиты информации; – типовые методы скрытия информации; – методы резервного копирования данных. 	<p>«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.</p> <p>«Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.</p>	<ul style="list-style-type: none"> • Решение ситуационной задачи Текущий контроль (проверочные работы, тесты) Промежуточный контроль (дифференцированный зачет)
---	---	--

5. ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ПРОГРАММЫ В ДРУГИХ РАБОЧИХ ОСНОВНЫХ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММАХ (РООП)

Квалификация "Программист"

Программист с помощью специальных математических моделей разрабатывает компьютерные программы. К настоящему моменту в сообществе этих специалистов можно выделить три группы: прикладные, системные и web-программисты. Именно от прикладных программистов зависит, насколько успешно и безопасно будет идти работа в компании, в которой задействованы современные технические устройства (будь то бухгалтерская программа или система пожаротушения). Деятельность системных программистов заключается в работе с системным программным обеспечением. Они могут заниматься разработкой, созданием, управлением операционных систем.

Квалификация "Разработчик веб и мультимедийных технологий"

Квалификация "Разработчик веб и мультимедийных технологий" Разработчики Web и мультимедийных приложений сочетают в своей работе дизайнерские и технические знания для проведения исследований, анализа, оценки, проектирования, программирования и изменения веб-сайтов и приложений, объединяющих текстовые, графические, мультипликационные, изобразительные, звуковые и видеоматериалы, а также другие интерактивные средства.

Разработчики:

Н.А. Назарова - преподаватель ГБПОУ «ЮУГК»

А.Ю. Скворцов - Руководитель отдела информационных технологий ЗАО ЮУИК «Трейд-Альянс»