Частное профессиональное образовательное учреждение
«Башкирский экономико-юридический колледж (БЭК)»

Утверждаю
Директор ЧПОУ "Башкирский
экономико-юридический колледж"

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
БЭК
Сертификат: 05BE73001CAECFA34D73F757F4D32A59
Владелец: КУЗЕЕВ ИСКАНДЕР ЭНГИЛЕВИЧ
Действителен: с 13.01.2022 до 13.04.2023

_____И.Э. Кузеев
"_____"_____2023 г.

РАБОЧАЯ ПРОГРАММА

учебной дисциплины Информационная безопасность

код, специальность 09.02.07 Информационные системы и программирование

Уфа
2023

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 09.02.07 Информационные системы и программирование

ОДОБРЕНО:
ПМК Компьютерных технологий
Протокол № 7
от « 20 » марта 2023г.
Председатель предметно-методической комиссии
_____ / Ю.В. Жаркова /

УТВЕРЖДЕНО:
Заместитель директора по учебной и методической работе
_____ / И.М. Ситдиков /

Составитель: Хамзина Д.В., преподаватель высшей категории

Рекомендовано методическим советом
Протокол № 6 от « 21 » марта 2023г.

СОДЕРЖАНИЕ

		стр.
1.	**ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**	4
2.	**СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**	5
3.	**УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**	10
4.	**КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ**	12

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

1.1. Место дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина «Информационная безопасность» относится к общепрофессиональному циклу.

Дисциплина введена за счет часов вариативной части с целью расширения основного вида деятельности выпускника в соответствии с запросами регионального рынка труда.

1.2. Цель и планируемые результаты освоения дисциплины:

Код ПК, ОК	Умения	Знания
ОК 1. ОК 2. ОК 4. ОК 5. ОК 9. ОК 10. ПК 4.1. ПК 4.4 ПК 11.6.	– *правильно и точно оценивать ситуацию в информационном мире;* – *применять правовые, организационные, технические и программные средства защиты информации;* – *создавать программные средства защиты информации*	– *настройки, эксплуатацию и обслуживание компонентов обеспечивающих информационную безопасность;* – *источники возникновения информационных угроз;* – *модели и принципы защиты информации от несанкционированного доступа;* – *методы антивирусной защиты информации;* – *состав и методы организационно-правовой защиты информации.*

1.3. Рекомендуемое количество часов на освоение программы дисциплины

максимальной учебной нагрузки обучающегося 66 часов, в том числе:

- обязательной аудиторной учебной нагрузки обучающегося 62 часа;
- самостоятельной работы обучающегося 4 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной деятельности	Объем часов
Объем образовательной программы	66
Объем работы обучающихся во взаимодействии с преподавателем	62
в том числе:	
- теоретическое обучение	42
- лабораторные работы(если предусмотрено)	-
- практические занятия(если предусмотрено)	20
- курсовая работа (проект) (если предусмотрено)	-
- самостоятельная работа	4
- промежуточная аттестация (дифференцированный зачет)	-

2.2. Тематические план и содержание учебной дисциплины «Информационная безопасность»

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Основные понятия и определения информационной безопасности.		**2**	
Тема 1.1. Введение. Основные сервисы безопасности. Модель сетевой безопасности	Понятие информационной безопасности. Пользоваться основными понятия информационной безопасности на практике. Информационная безопасность, угроза, атака. Сервисы безопасности. Использование сервисов безопасности на практике. Сервис безопасности, модель сетевой безопасности, злоумышленник, владелец информации, шифрование.	2	ОК 1., ОК 2., ПК 4.1
Раздел 2. Угрозы безопасности		**7**	
Тема 2.1. Основные определения. Классификация угроз.	Угрозы безопасности. Распознавание угроз безопасности. Внешняя угроза, внутренняя угроза, атака, уязвимость.	2	ОК 1., ОК 2., ОК 4.,ПК 4.1., ПК 11.6
	Самостоятельная работа: Определение угроз и уязвимости Вашего вымышленного предприятия (Реферат)	2	
Тема 2.2. Угрозы доступности. Угрозы целостности.	Угрозы доступности. Распознавание угроз доступности на практике. Угроза доступности, доступ, системный администратор, пользователь, пароль.	1	
	Практическое занятие 1. Создание учетных записей пользователей. Настройка политики IPSec.	2	
Раздел 3. Атаки		**9**	

Тема 3.1 Пассивные атаки. Активные атаки.	Пассивные атаки. Организация защиты систем от пассивных атак. Атака, конфиденциальность информации, целостность информации, доступность системы. Активные атаки. Организация защиты системы от активных атак. Атака, атакуемый объект, злоумышленник, конфиденциальность информации, целостность информации.	1	ОК 4., ОК 5., ОК 9., ОК 10., ПК 4.1., ПК 4.4., ПК 11.6.
Тема 3.2. Атаки на беспроводные сети.	Виды атак на беспроводные сети. Подключение принтера. Штриховое кодирование, виды штрих кодов, термический принтер, термотрансферный принтер.	2	
Тема .3.3. Уровни сетевых атак согласно модели OSI.	Уровни сетевых атак. Организация защиты от сетевых атак и применение их на практике. Сетевая атака, модель OSI, уровни модели OSI.	2	
	Практическое занятие 2. Настройка VPN - соединения.	2	
	Практическое занятие 3. Назначение основных портов TCP/IP.	2	
Раздел 4. Системы обнаружения вторжений		**8**	
Тема 4.1. Сигнатурные и поведенческие методы.	Методы обнаружения вторжений. Использование сигнатурных и поведенческих методов на практике. Система обнаружения вторжений, сигнатурный метод, поведенческий метод.	2	ОК 4., ОК 5., ОК 9.,ПК 4.1., ПК 4.4., ПК 11.6.
Тема 4.2. Сетевые и хостовые датчики.	Виды датчиков используемые в системах обнаружения вторжений. Использование сетевых и хостовых датчиков. Хост, сетевой датчик.	2	
Тема 4.3. Принцип работы систем обнаружения вторжений.	Принцип работы систем обнаружения вторжений. Организация работы с системой обнаружения вторжений. Система обнаружения вторжений, сетевые датчики, сигнатурный.	2	
	Практическое занятие 4. Работа с системой обнаружения вторжений.	2	
Раздел 5. Вредоносное программное обеспечение		**16**	
Тема 5.1. Вирусы и черви.	Виды вирусов. Использование антивирусного ПО. Вирус, черви, антивирусные программы, тело вируса.	2	ОК 2.,ОК 4., ОК 5., ОК 9., ПК 4.1., ПК 4.4., ПК 11.6.
Тема 5.2. Троянские программы, логические бомбы.	Троянские программы, логические бомбы. Использование антивирусных ПО. Троянская программа.	2	
Тема 5.3. Программно-технические методы обнаружения вирусов.	Методы обнаружения вирусов. Настраивание антивирусного ПО. Антивирус, эвристический анализ, операционная система.	2	
Тема 5.4. Защита файл-сервера,	Принципы защиты серверов. Организация работы с программными и	2	ОК 2.,ОК 4., ОК

почтового сервера, сервера баз данных. Сетевой центр управления антивирусами.	техническими средствами защиты серверов. Антивирус, файл-сервер, сервер баз данных, почтовый сервер.		5., ОК 9., ПК 4.1., ПК 4.4., ПК 11.6.
	Практическое занятие 5,6. Установка, настройка и работа с антивирусным программным обеспечением.	4	
	Практическое занятие 7,8.Установка, настройка и работа с программой Anti-Hacker.	4	
Раздел 6 Межсетевые экраны.		**4**	
Тема 6.1. Виды межсетевых экранов. Создание наборов правил для межсетевых экранов.	Принцип работы межсетевого экрана. Настраивание правил для межсетевого экрана. Межсетевой экран, модель OSI, правила для межсетевых экранов.	2	ОК 1., ОК 10., ПК 4.4
	Практическое занятие 9. Настройка встроенного брандмауэра Windows 7, 10.	2	
Раздел 7. Сканеры безопасности.		**4**	
Тема 7.1. Механизмы работы сканеров безопасности и методы их реализации. Этапы сканирования.	Принцип работы сканеров безопасности. Работа со сканером безопасности. Сканер безопасности, сканирование, зондирование. Этапы сканирования. Проведение анализа защищенности с помощью сканера безопасности. Сканер безопасности, уязвимость, отчет.	2	ОК 1., ПК 4.1., ПК 4.4.
	Практическое занятие 10. Настройка сканера безопасности. Проверка уязвимости системы. Анализ полученных данных.	2	
Раздел 8. Политика безопасности предприятия.		**2**	
Тема 8.1. Основные определения политики безопасности. Этапы создания политики безопасности.	Основные определения политики безопасности. Использование политики безопасности. Политика безопасности, злоумышленник, уязвимость, информация. Этапы создания политики безопасности. Создание политики безопасности. Политика безопасности, атака, защита, данные.	2	ОК 1., ОК 10., ПК 4.1., ПК 4.4.
Раздел 9. Аудит информационной безопасности.		**4**	
Тема 9.1. Активный аудит.	Понятие активного аудита. Проведение аудита. Аудит, активный аудит, проверка, уязвимость.	2	ОК 9., ПК 4.1., ПК 4.4., ПК 11.6.
Тема 9.2. Экспертный аудит. Аудит на соответствие стандартам.	Понятие экспертного аудита. Проведение аудита. Аудит, экспертный аудит, аудит на соответствие стандартам, проверка, уязвимость.	2	
Раздел 10. Безопасность в ОС		**4**	

Windows 7, 10 и Windows Server 2012			
Тема 10.1. Безопасность в Windows 7, 10	Каким образом реализуются требования безопасности в Windows 7, 10. Организация настройки политики безопасности в Windows 7, 10. Политика безопасности, пароли, учетные записи пользователей.	2	ОК 2., ОК 5., ОК 9., ПК 4.1., ПК 4.4., ПК 11.6.
Тема 10.2. Настройка безопасности в Windows Server 2012	Реализация требований безопасности в Windows Server 2012. Организация настройки политики безопасности в Windows Server 2012. Клиент-сервер, администратор, шифрование, политика безопасности, пароли, учетные записи пользователей.	2	
Раздел 11. Законодательный уровень информационной безопасности.		**3**	
Тема 11.1. Обзор законодательства РФ. Обзор законодательства зарубежных стран.	Законодательство РФ в области информационной безопасности. Использование законов. Информационная безопасность, административные меры, законодательные меры. Законодательство зарубежных стран в области информационной безопасности. Информационная безопасность, административные меры, законодательные меры.	2	ОК 2., ОК 5., ОК 9., ПК 4.1., ПК 4.4., ПК 11.6.
	Самостоятельная работа. Изучение законов РФ в области информационной безопасности. (Реферат).	1	
Раздел 12. Объектно-ориентированный подход к информационной безопасности.		**3**	
Тема 12.1. Основные понятия объектно-ориентированного подхода к информационной безопасности. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.	Основные понятия. Применение на практике объектно-ориентированного подхода. Объектно-ориентированный подход, класс, объект, инкапсуляция, наследование, полиморфизм. Каким образом применяется объектно-ориентированный подход. Применение объектно-ориентированного подхода по отношению к защищаемым системам.	2	ОК 2.,ОК 4., ОК 5., ОК 9., ПК 4.1., ПК 4.4., ПК 11.6.
	Самостоятельная работа. Объектно-ориентированный подход, информационная система, декомпозиция. (Поиск информации в Интернет).	1	
	Всего:	**66**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия лаборатории программного обеспечения и сопровождения компьютерных систем.

Оборудование лаборатории:

- Автоматизированные рабочие места на 12 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

Основная литература:

1. Суворова, Г. М. Основы информационной безопасности : учебное пособие для СПО / Г. М. Суворова. — Саратов : Профобразование, 2021. — 214 с. — ISBN 978-5-4488-1294-1. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/108005.
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 // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/102207.

Дополнительная литература:

1. Шаньгин, В. Ф. Информационная безопасность и защита информации: учебник / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87995.
2. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности : учебное пособие для СПО / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Саратов : Профобразование, 2021. — 431 с. — ISBN 978-5-4488-1015-2. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/102208

Интернет-ресурсы:

1. Информационный портал [Электронный ресурс]. Режим доступа: https://habr.com.

2. Национальный открытый университет [Электронный ресурс]. Режим доступа: https://www.intuit.ru/.

3. Журнал "Компьютер Пресс" https://compress.ru/.

4. Справочная правовая система КонсультатПлюс. [Электронный ресурс] – режим доступа: http://www.consultant.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения студентами индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Критерии оценки**	**Формы и методы контроля и оценки результатов обучения**
Умения:		
− правильно и точно оценивать ситуацию в информационном мире	«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.	практические работы, дифференцированный зачет.
− применять правовые, организационные, технические и программные средства защиты информации		практические занятия, внеаудиторная самостоятельная работа, дифференцированный зачет.
− создавать программные средства защиты информации		практические занятия, дифференцированный зачет.
Знания:		
− настройки, эксплуатацию и обслуживание компонентов обеспечивающих информационную безопасность		практические занятия, дифференцированный зачет.
− источники возникновения информационных угроз		практические занятия, дифференцированный зачет.
− модели и принципы защиты информации от несанкционированного доступа		практические занятия, дифференцированный зачет.
− методы антивирусной защиты информации		внеаудиторная самостоятельная работа, дифференцированный зачет.
− состав и методы организационно-правовой защиты информации		практические занятия, дифференцированный зачет.