профессиональная образовательная организация ассоциация
«Региональный финансово-экономический техникум»

Цикловая комиссия математических, естественно-научных и экономических дисциплин

Утверждаю
зам. директора по УР
_____ Ю.И. Петренко
«26» июня 2020 г.

Рабочая программа учебной дисциплины

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

специальности **09.02.05 Прикладная информатика (по отраслям)**

(заочная форма обучения)

Курск 2020

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования (далее – СПО) 09.02.05 «Прикладная информатика (по отраслям)» (базовой подготовки), утвержденного приказом Министерства образования и науки Российской Федерации от 13 августа 2014 года № 1001.

Составитель: _____ Смецкой А.С., преподаватель цикловой комиссии математических, естественно-научных и экономических дисциплин

Рабочая программа утверждена на заседании цикловой комиссии математических, естественно-научных и экономических дисциплин, протокол № 10 от «26» июня 2020 г.

Председатель цикловой комиссии _____В.Н. Бутова

Изменения в рабочей программе по учебной дисциплине
«Информационная безопасность»
на 2021/2022 уч. г.

УТВЕРЖДАЮ

Зам. директора по учебной работе

_____ Ю.И. Петренко

«25» июня 2021 г.

В рабочую программу вносятся следующие изменения:
1) внесены изменения в список основной литературы;
2) внесены изменения в перечень вопросов для подготовки к зачету.

Рабочая программа утверждена на заседании цикловой комиссии математических, естественно-научных и экономических дисциплин, протокол № 8 от «25» июня 2021 г.

Председатель цикловой комиссии _____ В.Н. Бутова

Изменения в рабочей программе
по учебной дисциплине
«Информационная безопасность»
на 2022-2023 уч. год

УТВЕРЖДАЮ

Зам. директора по учебной работе

_____ Ю.И. Петренко

«26» августа 2022 г.

В рабочую программу вносятся следующие изменения:

1) внесены изменения в перечень в список дополнительной литературы.

Рабочая программа утверждена на заседании цикловой комиссии математических, естественно-научных и экономических дисциплин, протокол № 1 от «26» августа 2022 г.

Председатель цикловой комиссии _____ В.Н. Бутова

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

«Информационная безопасность»

1.1. Область применения программы:

Рабочая программа дисциплины является частью программы подготовки специалистов среднего звена по специальности СПО в соответствии с ФГОС специальности 09.02.05 Прикладная информатика (по отраслям) (базовой подготовки) в части освоения основного вида профессиональной деятельности (ОПД): **Информационная безопасность.**

1.2. Место дисциплины в структуре программы подготовки специалистов среднего звена: является вариативной дисциплиной математического и общего естественнонаучного учебного цикла.

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

Целью изучения дисциплины «Информационная безопасность» является формирование знаний и умений, которые образуют теоретический и практический фундамент, необходимый для построения и анализа безопасных информационных систем и технологий.

В результате освоения учебной дисциплины обучающийся должен **уметь**:

- выполнять операции в алгебре вычетов (У-1);
- применять простейшие криптографические шифры для шифрования текстов (У-2);
- применять организационные, правовые, технические и программные средства защиты информации (У-3);
- создавать программные средства защиты информации (У-4).

В результате освоения учебной дисциплины обучающийся должен **знать**:

- основные понятия информационной безопасности (З-1);
- источники возникновения информационных угроз (З-2);
- модели и принципы защиты информации от несанкционированного доступа (З-3);
- методы антивирусной защиты информации (З-4);
- состав и методы организационно-правовой защиты информации (З-5).

1.4. Перечень формируемых компетенций в результате освоения учебной дисциплины:

Код	Наименование результата обучения
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-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	Обрабатывать статический информационный контент.
ПК 1.3	Осуществлять подготовку оборудования к работе.
ПК 2.1	Осуществлять сбор и анализ информации для определения потребностей клиента.
ПК 2.3	Проводить отладку и тестирование программного обеспечения отраслевой направленности.
ПК 2.4	Проводить адаптацию отраслевого программного обеспечения.
ПК 4.5	Определять риски проектных операций.

1.5. Рекомендуемое количество часов на освоение программы учебной дисциплины:

максимальной учебной нагрузки обучающегося 186 час., в том числе:
обязательной аудиторной учебной нагрузки обучающегося 38 часов;
самостоятельной работы обучающегося 148 часов.

2. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	186
Обязательная аудиторная учебная нагрузка (всего)	**38**
в том числе:	
обзорно-установочные занятия	26
лабораторно-практические занятия	12
Самостоятельная работа обучающегося (всего)	**148**
Итоговая аттестация проводится в форме *зачета*	

2.2. Тематический план и содержание тем учебной дисциплины «Информационная безопасность»

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Общие положения: понятие информационной безопасности			
Тема 1.1. Средства защиты от несанкционированного доступа	**Содержание учебного материала** Средства авторизации. Мандатное управление доступом. Избирательное управление доступом. Управление доступом на основе ролей. Журналирование.	2	1, 2
	Самостоятельная работа. 1. Проработка учебного материала. 2. Подбор и изучение нормативных актов, литературы, юридической практики.	22	
Тема 1.2. Системы анализа и моделирования информационных потоков	**Содержание учебного материала** Системы анализа и моделирования информационных потоков (CASEсистемы). Системы мониторинга. Системы обнаружения и предотвращения вторжений (IDS/IPS). Системы предотвращения утечек конфиденциальной информации (DLP-системы).	4	1,2
	Самостоятельная работа. 1. Проработка учебного материала. 2. Составление схем, таблиц.	22	
Раздел 2. Сетевые атаки и способы защиты			
Тема 2.1. Системы мониторинга сетей	**Содержание учебного материала** Анализаторы протоколов. Межсетевые экраны. Виды систем обнаружения вторжений. Пассивные и активные системы обнаружения вторжений. Сравнение СОВ и межсетевого экрана. История разработок СОВ. Свободно распространяемые СОВ. Коммерческие СОВ.	4	2
	Самостоятельная работа. 1. Проработка учебного материала. 2. Подготовка доклада о системе мониторинга сетей.	20	
Тема 2.2. Антивирусные средства.	**Содержание учебного материала** Антивирусная программа. Хронология компьютерных вирусов и червей. Целевые платформы антивирусного ПО. Антивирусные продукты для ОС семейства Windows. Антивирусные продукты для ОС семейства *NIX (к данному семейству относятся ОС BSD, Linux и др.). Антивирусные продукты для ОС семейства MacOS.	4	2

	Практическое занятие № 1 Анализ различных сетевых атак	4	
	Самостоятельная работа. 1. Проработка учебного материала. 2. Поиск материала по заданной теме.	20	
Раздел 3. Основы криптографии			
Тема 3.1. Криптографические средства	**Содержание учебного материала** Шифрование; Цифровая подпись. Криптографические атаки. Криптографические хеш-функции. Криптографическое программное обеспечение. Стандарты криптографии	4	2
	Практическое занятие № 2 Государственные криптографические стандарты.	4	
	Самостоятельная работа. 1. Проработка учебного материала. 2. Анализ алгоритмов.	22	
Тема 3.2. Системы аутентификации	**Содержание учебного материала** Идентификация личности. Менеджеры паролей. Одноразовый пароль. Односторонняя функция с потайным входом. Бесконтактная карта Биометрические системы аутентификации.	4	2
	Самостоятельная работа. 1. Проработка учебного материала. 2. Составление схем, таблиц.	22	
Тема 3.3. Средства предотвращения взлома корпусов и краж оборудования.	**Содержание учебного материала** Кабины и шкафы модульные серверные. Оборудование для депозитариев. Системы противокражные. Средства предотвращения взлома корпусов. Устройства антивандальные.	4	2
	Практическое занятие № 3 Модульная арифметика. Сравнимость чисел по имитационной ситуации	4	
	Самостоятельная работа. 1. Проработка учебного материала. 2. Выполнение расчетов	20	
	Всего	**186**	

3. КОМПЛЕКТ КОНТРОЛЬНО–ОЦЕНОЧНЫХ СРЕДСТВ

Смотри приложение №1.

4. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

4.1. Требования к минимальному материально-техническому обеспечению

1. Аудиторная база (лекционная аудитория, аудитория для проведения практических занятий, виртуальные классные комнаты на портале РФЭТ)
2. Организационно-технические средства и аудиовизуальный фондовый материал, мультимедийное оборудование.
3. Комплекты видеофильмов, аудиокниг, CD-дисков по проблемам дисциплины.
4. Интернет.
5. Информационно-правовая система «Консультант +»

4.2. Информационное обеспечение обучения

Основная литература

1. Информационная безопасность и защита информации: учебное пособие. —311 с. — Электронное издание. 978-5-374-00301-7 Баранова, Е. К. 2017 г. М. : ЕАОИ

Дополнительная литература

1. Алешенков М. Основы национальной безопасности/М.Алешенков /Основы безопасности жизни.-2015.-№11.-С.5-10.
2. Андреев Э. М., Миронов А.В. Социальные проблемы интеллектуальной уязвимости и информационной безопасности //Социально-гуманитарные знания.-2019.-№4.-С.169-180.
3. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2012.— 208 с.— ISBN 5-8459-0323-8, ISBN 1-57870-264-X.
4. Брандман Э. М. Цивилизационные императивы и приоритеты информационной безопасности общества/Э.М.Брандман //Философия и общество.-2006.-№3.-С.60-77..-Предпринимательство, с.131-144.
5. Галатенко В. А. Стандарты информационной безопасности.— М.: Интернет-университет информационных технологий, 2016.— 264 с.— ISBN 5-9556-0053-1.
6. Галицкий А. В., Рябко С. Д., Шаньгин В. Ф. Защита информации в сети— анализ технологий и синтез решений. М.: ДМК Пресс, 2018.— 616 с.— ISBN 5-94074-244-0.
7. Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В.Информационная безопасность открытых систем. В 2-х тт.
8. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2017.— 176 с.— ISBN 978-985-463-258-2.

9. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. М.: 2017.— 428 с.— ISBN 5-93598-030-4.
10. Петренко С. А. Управление информационными рисками. М.: Компания АйТи; ДМК Пресс, 2014.— 384 с.— ISBN 5-98453-001-5.
11. Петренко С. А., Курбатов В.А. Политики информационной безопасности.— М.: Компания АйТи, 2016.— 400 с.— ISBN 5-98453-024-4.
12. Поляков В. П. Практическое занятие по изучению вопросов информационной безопасности/В.П.Поляков //Информатика и образование.-2006.-№11.-С.75-80.
13. Поляков В.П. Информационная безопасность в курсе информатики /В.П.Поляков //Информатика и образование.-2006.-№10.-С.116-119.
14. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2011.— 272 с.— ISBN 978-5-388-00069-9.
15. Семенова З. В. Углубленное изучение темы "Защита данных в информационных системах" //Информатика и образование.-2014.-№1.-С.32-39.

Интернет ресурсы:

1. Электронная библиотека Регионального финансово-экономического техникума http://students.rfet.ru/a/students/library.jspx
2. Электронная библиотека Регионального финансово-экономического института /http://lib2.rfei.ru/
3. Электронно - библиотечная система iBooks http://ibooks.ru/
4. Федеральный портал «Российское образование» http://www.edu.ru/
5. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» http://school-collection.edu.ru/
6. Российская Государственная Библиотека http://www.rsl.ru/
7. Фундаментальная библиотека СПбГПУ – http://www.unilib.neva.ru/rus/lib/

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСНОВЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения:	
выполнять операции в алгебре вычетов (У-1);	Оценка выполнения контрольного задания. Оценка выполнения тестовых заданий. Оценка выполнения практических работ. Оценка выполнения самостоятельной работы. Зачет.
применять простейшие криптографические шифры для шифрования текстов (У-2);	
применять организационные, правовые, технические и программные средства защиты информации (У-3);	
создавать программные средства защиты информации (У-4);	
Знания:	
основные понятия информационной безопасности (З-1);	
источники возникновения информационных угроз (З-2);	
модели и принципы защиты информации от несанкционированного доступа (З-3);	
методы антивирусной защиты информации (З-4);	
состав и методы организационно-правовой защиты информации (З-5).	