Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Мишкина Л. В.
Должность: директор
Дата подписания: 15.03.2022 13:59:49
Уникальный программный ключ:
8816e64d7bbb2e4c0905580453a91cd7fed713c59

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА ДАННЫХ

1.1. Область применения программы

Рабочая программа учебной дисциплины Кибербезопасность и защита данных является частью основной профессиональной образовательной программы среднего профессионального образования – программы подготовки специалистов среднего звена по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Дисциплина входит в общеобразовательный цикл и относится к дисциплинам по выбору.

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

Цель программы: ознакомление с базовыми понятиями кибербезопасности и защиты данных, подготовка студентов к обеспечению безопасности в сети Интернет, защите личных данных, развитие компетенций цифровой экономики для активной трудовой деятельности в цифровом обществе.

В результате изучения учебной дисциплины «Кибербезопасность и защита данных» на уровне среднего общего образования:

В результате освоения учебной дисциплины обучающийся должен уметь:

- формулировать принципы и строить модель угроз и нарушителей по методике ФСТЭК;
- описывать риски и угрозы персональных данных;
- формулировать и проектировать политику информационной безопасности организации (предприятия);
- ориентироваться в современных угрозах и факторах риска в условиях цифровой трансформации общества и государства;
- противодействовать угрозам кибербезопасности с использованием аппаратных и программных средств защиты информации;
- работать с программным обеспечением с соблюдением действующих требований по защите информации;
- оценивать риски, связанные с осуществлением угроз безопасности в отношении компьютерных систем;
- работать с биометрическими системами идентификации и аутентификации;
- настроить программное обеспечение с соблюдением требований по защите информации;
- осуществлять проверки функционирования встроенных средств защиты информации программного обеспечения;

В результате освоения учебной дисциплины обучающийся должен знать:

- основные понятия кибербезопасности, информационной безопасности и персональных данных;
- сущность и содержание понятия информационной безопасности,

характеристики ее составляющих;

- источники угроз информационной безопасности и меры по их предотвращению;
- особенности источников угроз информационной безопасности, связанных с эксплуатацией программного обеспечения;
- основные понятия о биометрических системах защиты данных;
- уязвимости компьютерных систем и сетей;
- правовые основы обеспечения кибербезопасности;
- нормативные правовые акты в области защиты информации;
- организационные, технические и правовые меры по защите информации;
- принципы работы и правила эксплуатации программно-аппаратных средств защиты данных.

Указываются требования к умениям и знаниям в соответствии с перечисленными в п. 1.ФГОСов по специальностям / профессиям

1.4. Количество часов на освоение программы дисциплины:

обязательная аудиторная учебная нагрузка обучающегося 39 часов;