

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Агаберди Раиса Левонян

Должность: ректор

Дата подписания: 03.06.2022 08:15:37

Уникальный программный ключ:

4237c7ccb9b9e111bbaf1f4fcd9201d015c4dbaa123ff774747307b9b9fcb8

Негосударственное аккредитованное не коммерческое частное образовательное учреждение
высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

УТВЕРЖДАЮ

Проректор по учебной работе,
доцент Н. И. Севрюгина
28 марта 2022 г.

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Программно-аппаратные и технические средства защиты информации

Специальность 10.02.01 Организация и технология защиты информации

Нормативный срок освоения ОПОП ППСЗ 3г. 10 мес.

Уровень подготовки базовый

Наименование квалификации техник по защите информации

Место учебной дисциплины в структуре основной профессиональной образовательной программы: Профессиональный цикл. Профессиональные модули

Требования к результатам освоения модуля:

В результате изучения профессионального модуля обучающийся должен:

иметь практический опыт:

- участия в эксплуатации систем и средств защиты информации защищаемых объектов;
- применения технических средств защиты информации;
- выявления возможных угроз информационной безопасности объектов защиты;

уметь:

- работать с техническими средствами защиты информации;
- работать с защищенными автоматизированными системами;
- передавать информацию по защищенным каналам связи;
- фиксировать отказы в работе средств вычислительной техники;

знать:

- виды, источники и носители защищаемой информации;
- источники опасных сигналов;
- структуру, классификацию и основные характеристики технических каналов утечки информации;
- классификацию технических разведок и методы противодействия им;
- методы и средства технической защиты информации;
- методы скрытия информации;
- программно-аппаратные средства защиты информации;
- структуру подсистемы безопасности операционных систем и выполняемые ею функции;

- средства защиты в вычислительных сетях;
- средства обеспечения защиты информации в системах управления базами данных;
- критерии защищенности компьютерных систем;
- методики проверки защищенности объектов информатизации на соответствие требованиям нормативных правовых актов.

Перечень формируемых компетенций:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

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 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

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.

ОК 10. Применять математический аппарат для решения профессиональных задач.

ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности.

ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.

ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.

ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.

ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.

ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.

Программой профессионального модуля предусмотрены следующие виды учебной работы:

Вид учебной деятельности	Объем часов всего
Максимальная учебная нагрузка (всего)	728
Обязательная аудиторная учебная нагрузка (всего)	488
в том числе:	
теоретическое обучение	244
практические занятия	214
Самостоятельная работа студента (всего)	240
Практика (виды практики в неделях/часах): учебная	2/72
производственная (по профилю специальности)	3/1/2/126
Курсовая работа	30
Вид промежуточной аттестации – квалиф. экзамен	8 семестр