Негосударственное аккредитование некоммерческое частное образовательное учреждение

Академия маркетинга и социально-информационных технологий – ИМСИТ

(г. Краснодар)

УТВЕРЖДАЮ
Ректор Академии ИМСИТ,
профессор
Агабекян Р.Л.
«13» апреля 2020 г.

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Специальность 10.02.01 Организация и технология защиты информации

Нормативный срок освоения ОПОП ППССЗ 3г. 10 мес.

Уровень подготовки Базовый

Наименования квалификации Техник по защите информации

ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта	В результате изучения профессионального модуля обучающийся должен: иметь практический опыт: – использования физических средств защиты объекта; – применения физических средств контроля доступа на объект; – ведения текущей работы исполнителей с конфиденциальной информацией; В результате освоения профессионального модуля обучающийся должен **уметь**: – организовывать охрану персонала, территорий, зданий, помещений и продукции организаций; – пользоваться аппаратурой систем контроля доступа; – выделять зоны доступа по типу и степени конфиденциальности работ; – определять порядок организации и проведения рабочих совещаний; – использовать методы защиты информации в рекламной и выставочной деятельности; – использовать критерии подбора и расстановки сотрудников подразделений защиты информации; – организовывать работу с персоналом, имеющим доступ к

	конфиденциальной информации; – проводить инструктаж персонала по организации работы с конфиденциальной информацией; – контролировать соблюдение персоналом требований режима защиты информации; В результате освоения профессионального модуля обучающийся должен **узнать**: – виды и способы охраны объекта; – особенности охраны персонала организации; – основные направления и методы организации режима и охраны объекта; – разрешительную систему доступа к конфиденциальной информации; – принципы действия аппаратуры систем контроля доступа; – принципы построения и функционирования биометрических систем безопасности; – требования и особенности оборудования режимных помещений; – требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров; – требования режима защиты информации при приеме в организации посетителей; – организацию работы при осуществлении международного сотрудничества; – требования режима защиты информации в процессе рекламной деятельности; – требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати; – задачи, функции и структуру подразделений защиты информации; – принципы, методы и технологию управления подразделений защиты информации; – методы проверки персонала по защите информации; – процедуру служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.
ПМ.02 Организация и технология работы с конфиденциальными документами	В результате изучения профессионального модуля обучающийся должен: иметь практический опыт: – ведения учета и оформления бумажных и машинных носителей конфиденциальной информации; – работы с информационными системами электронного документооборота; В результате освоения профессионального модуля обучающийся должен **уметь**: – использовать в профессиональной деятельности нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации,

	Федеральной службы по техническому и экспортному контролю в данной области; – разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации; – документировать ход и результаты служебного расследования; – определять состав документируемой конфиденциальной информации; – подготавливать, издавать и учитывать конфиденциальные документы; – составлять номенклатуру конфиденциальных дел; – формировать и оформлять конфиденциальные дела; – организовывать и вести конфиденциальное делопроизводство, в том числе с использованием вычислительной техники; – использовать системы электронного документооборота; В результате освоения профессионального модуля обучающийся должен **узнать**: – основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области; – правовые основы защиты конфиденциальной информации по видам тайны; – порядок лицензирования деятельности по технической защите конфиденциальной информации; – правовые основы деятельности подразделений защиты информации; – правовую основу допуска и доступа персонала к защищаемым сведениям; – правовое регулирование взаимоотношений администрации и персонала в области защиты информации; – систему правовой ответственности за утечку информации и утрату носителей информации; – правовые нормы в области защиты интеллектуальной собственности; – порядок отнесения информации к разряду конфиденциальной информации; – порядок разработки, учета, хранения, размножения и уничтожения конфиденциальных документов; – организацию конфиденциального документооборота; – технологию работы с конфиденциальными документами; – организацию электронного документооборота
ПМ,03 Программно-аппаратные и технические средства информации	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;

	В результате освоения профессионального модуля обучающийся должен **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; В результате освоения профессионального модуля обучающийся должен **узнать**: – 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.
ПМ.04 Выполнение по одной или нескольким профессиям рабочих ,должностям служащих	В результате изучения профессионального модуля обучающийся должен: иметь практический опыт: В результате освоения профессионального модуля обучающийся должен **уметь**: – выполнять ввод-вывод информации с носителей данных, каналов связи; – готовить к работе вычислительную технику и периферийные устройства; – осуществлять поиск и устранение сбоев программ ЭВМ; – пользоваться клавиатурой персонального компьютера; – работать в операционной системе WINDOWS; – работать в текстовом редакторе WORD; – работать с электронными таблицами EXCEL; – работать с базой данных ACCESS; – осуществлять ввод, редактирование и оформление информации; – работать с программами по архивации данных; – проверять файлы, диски и папки на наличие вирусов; – использовать средства защиты информации от несанкционированного доступа и случайных воздействий; – владеть правовыми аспектами информационной деятельности; – соблюдать санитарно-гигиенические требования, нормы и

	правила по охране труда. В результате освоения профессионального модуля обучающийся должен **узнать**: – архитектуру ЭВМ; – устройство системного блока и его основных узлов; – приемы ввода-вывода информации в ЭВМ; – правила включения, перезагрузки и выключения компьютера и периферийных устройств; – правила поиска и устранения сбоев в работе программ ЭВМ; – функции и группы клавиш на клавиатуре персонального компьютера, варианты клавиатурных комбинаций. Слепой метод набора текста; – структуру, свойства и возможности операционной системы Windows; – правила пользования текстовым редактором Word; – правила пользования электронными таблицами Excel; – правила пользования базами данных Access; – правила архивации и разархивации файлов; – разновидности антивирусных программ, принципы их действия, способы настройки и порядок работы с ними; – правовые аспекты информационной деятельности; – санитарно-гигиенические требования к организации рабочего места; правила техники безопасности и противопожарной защиты.

Перечень формируемых общих компетенций:

ОК.01 Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК.02 Понимать и анализировать вопросы ценностно-мотивационной сферы.

ОК.03 Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК.04 Принимать решения в стандартных и нестандартных ситуациях, в том числе ситуациях риска, и нести за них ответственность.

ОК.05 Проявлять психологическую устойчивость в сложных и экстремальных ситуациях, предупреждать и разрешать конфликты в
процессе профессиональной деятельности.

ОК.06 Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач,
профессионального и личностного развития.

ОК.07 Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК.08 Правильно строить отношения с коллегами, с различными категориями граждан, в том числе с представителями различных
национальностей и конфессий.

ОК.09 Устанавливать психологический контакт с окружающими.

ОК.10 Адаптироваться к меняющимся условиям профессиональной деятельности.

Перечень формируемых профессиональных компетенций:

ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта	ПК 1.1. Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации. ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте. ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации. ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности. ПК 1.5. Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации. ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий. ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите. ПК 1.8. Проводить контроль соблюдения персоналом требований режима защиты информации. ПК 1.9. Участвовать в оценке качества защиты объекта.
ПМ.02 Организация и технология работы с конфиденциальными документами	ПК 2.1. Участвовать в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации. ПК 2.2. Участвовать в организации и обеспечивать технологию ведения делопроизводства с учетом конфиденциальности информации. ПК 2.3. Организовывать документооборот, в том числе электронный, с учетом конфиденциальности информации. ПК 2.4. Организовывать архивное хранение конфиденциальных документов. ПК 2.5. Оформлять документацию по оперативному управлению средствами защиты информации и персоналом. ПК 2.6. Вести учет работ и объектов, подлежащих защите. ПК 2.7. Подготавливать отчетную документацию, связанную с эксплуатацией средств контроля и защиты информации. ПК 2.8. Документировать ход и результаты служебного

	расследования. ПК 2.9. Использовать нормативные правовые акты, нормативно-методические документы по защите информации.
ПМ,03 Программно-аппаратные и технические средства информации	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.
ПМ.04 Выполнение по одной или нескольким профессиям рабочих ,должностям служащих	ПК 4.1. Участвовать в разработке организационной структуры комплексной системы защиты информации (далее - КСЗИ). ПК 4.2. Участвовать в оценке технико-экономического уровня и эффективности организации КСЗИ. ПК 4.3. участвовать в подготовке заданий на реализацию КСЗИ. ПК 4.4. Организовывать и планировать работу малых коллективов исполнителей.

Количество часов , отводимое на учебную практику

Всего: 14 неделя, 504 часов