

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Агабекян Раиса Левоновна

Должность: ректор

Дата подписания: 17.12.2021 15:24:58

Уникальный программный ключ:

4237c7ccb9b9e111bbaf1f4fcda9201d015c4dbaa123ff774747307b9b9fcb7

Негосударственное аккредитованное не коммерческое частное образовательное учреждение

Академия маркетинга и социально-информационных технологий – ИМСИТ

(г. Краснодар)



Агабекян Р.Л.

«13» апреля 2020 г.

## АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

**Специальность** 10.02.01 Организация и технология защиты информации

**Нормативный срок освоения ОПОП ШССЗ** 2г. 10 мес.

**Уровень подготовки** Базовый

**Наименования квалификации** Техник по защите информации

<p>ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта</p>	<p>В результате изучения профессионального модуля обучающийся должен: иметь практический опыт:</p> <ul style="list-style-type: none"><li>– использования физических средств защиты объекта;</li><li>– применения физических средств контроля доступа на объект;</li><li>– ведения текущей работы исполнителей с конфиденциальной информацией;</li></ul> <p>В результате освоения профессионального модуля обучающийся должен <b>уметь</b>:</p> <ul style="list-style-type: none"><li>– организовывать охрану персонала, территорий, зданий, помещений и продукции организаций;</li><li>– пользоваться аппаратурой систем контроля доступа;</li><li>– выделять зоны доступа по типу и степени конфиденциальности работ;</li><li>– определять порядок организации и проведения рабочих совещаний;</li><li>– использовать методы защиты информации в рекламной и выставочной деятельности;</li><li>– использовать критерии подбора и расстановки сотрудников подразделений защиты информации;</li><li>– организовывать работу с персоналом, имеющим доступ к</li></ul>
---	---

	<p>конфиденциальной информации;</p> <ul style="list-style-type: none"> <li>– проводить инструктаж персонала по организации работы с конфиденциальной информацией;</li> <li>– контролировать соблюдение персоналом требований режима защиты информации;</li> </ul> <p>В результате освоения профессионального модуля обучающийся должен <b>узнать</b>:</p> <ul style="list-style-type: none"> <li>– виды и способы охраны объекта;</li> <li>– особенности охраны персонала организации;</li> <li>– основные направления и методы организации режима и охраны объекта;</li> <li>– разрешительную систему доступа к конфиденциальной информации;</li> <li>– принципы действия аппаратуры систем контроля доступа;</li> <li>– принципы построения и функционирования биометрических систем безопасности;</li> <li>– требования и особенности оборудования режимных помещений;</li> <li>– 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;</li> <li>– организацию работы при осуществлении международного сотрудничества;</li> <li>– требования режима защиты информации в процессе рекламной деятельности;</li> <li>– требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати;</li> <li>– задачи, функции и структуру подразделений защиты информации;</li> <li>– принципы, методы и технологию управления подразделений защиты информации;</li> <li>– методы проверки персонала по защите информации;</li> <li>– процедуру служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.</li> </ul>
<p>ПМ.02 Организация и технология работы с конфиденциальными документами</p>	<p>В результате изучения профессионального модуля обучающийся должен: иметь практический опыт:</p> <ul style="list-style-type: none"> <li>– ведения учета и оформления бумажных и машинных носителей конфиденциальной информации;</li> <li>– работы с информационными системами электронного документооборота;</li> </ul> <p>В результате освоения профессионального модуля обучающийся должен <b>уметь</b>:</p> <ul style="list-style-type: none"> <li>– использовать в профессиональной деятельности нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации,</li> </ul>

	<p>Федеральной службы по техническому и экспортному контролю в данной области;</p> <ul style="list-style-type: none"> <li>– разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации;</li> <li>– документировать ход и результаты служебного расследования;</li> <li>– определять состав документируемой конфиденциальной информации;</li> <li>– подготавливать, издавать и учитывать конфиденциальные документы;</li> <li>– составлять номенклатуру конфиденциальных дел;</li> <li>– формировать и оформлять конфиденциальные дела;</li> <li>– организовывать и вести конфиденциальное делопроизводство, в том числе с использованием вычислительной техники;</li> <li>– использовать системы электронного документооборота;</li> </ul> <p>В результате освоения профессионального модуля обучающийся должен <b>узнать</b>:</p> <ul style="list-style-type: none"> <li>– 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;</li> <li>– правовые основы защиты конфиденциальной информации по видам тайны; – порядок лицензирования деятельности по технической защите конфиденциальной информации;</li> <li>– правовые основы деятельности подразделений защиты информации; – правовую основу допуска и доступа персонала к защищаемым сведениям;</li> <li>– правовое регулирование взаимоотношений администрации и персонала в области защиты информации;</li> <li>– систему правовой ответственности за утечку информации и утрату носителей информации;</li> <li>– правовые нормы в области защиты интеллектуальной собственности;</li> <li>– порядок отнесения информации к разряду конфиденциальной информации;</li> <li>– порядок разработки, учета, хранения, размножения и уничтожения конфиденциальных документов;</li> <li>– организацию конфиденциального документооборота;</li> <li>– технологию работы с конфиденциальными документами;</li> <li>– организацию электронного документооборота</li> </ul>
<p>ПМ,03 Программно-аппаратные и технические средства информации</p>	<p>В результате изучения профессионального модуля обучающийся должен: иметь практический опыт:</p> <ul style="list-style-type: none"> <li>– участия в эксплуатации систем и средств защиты информации защищаемых объектов;</li> <li>– применения технических средств защиты информации;</li> <li>– выявления возможных угроз информационной безопасности объектов защиты;</li> </ul>

	<p>В результате освоения профессионального модуля обучающийся должен <b>уметь</b>:</p> <ul style="list-style-type: none"> <li>– работать с техническими средствами защиты информации;</li> <li>– работать с защищенными автоматизированными системами;</li> <li>– передавать информацию по защищенным каналам связи;</li> <li>– фиксировать отказы в работе средств вычислительной техники;</li> </ul> <p>В результате освоения профессионального модуля обучающийся должен <b>узнать</b>:</p> <ul style="list-style-type: none"> <li>– виды, источники и носители защищаемой информации;</li> <li>– источники опасных сигналов;</li> <li>– структуру, классификацию и основные характеристики технических каналов утечки информации;</li> <li>– классификацию технических разведок и методы противодействия им;</li> <li>– методы и средства технической защиты информации;</li> <li>– методы скрытия информации;</li> <li>– программно-аппаратные средства защиты информации;</li> <li>– структуру подсистемы безопасности операционных систем и выполняемые ею функции;</li> <li>– средства защиты в вычислительных сетях;</li> <li>– средства обеспечения защиты информации в системах управления базами данных;</li> <li>– критерии защищенности компьютерных систем;</li> <li>– методики проверки защищенности объектов информатизации на соответствие требованиям нормативных правовых актов.</li> </ul>
<p>ПМ.04 Выполнение по одной или нескольким профессиям рабочих ,должностям служащих</p>	<p>В результате изучения профессионального модуля обучающийся должен: иметь практический опыт:</p> <p>В результате освоения профессионального модуля обучающийся должен <b>уметь</b>:</p> <ul style="list-style-type: none"> <li>– выполнять ввод-вывод информации с носителей данных, каналов связи;</li> <li>– готовить к работе вычислительную технику и периферийные устройства;</li> <li>– осуществлять поиск и устранение сбоев программ ЭВМ;</li> <li>– пользоваться клавиатурой персонального компьютера;</li> <li>– работать в операционной системе WINDOWS;</li> <li>– работать в текстовом редакторе WORD;</li> <li>– работать с электронными таблицами EXCEL;</li> <li>– работать с базой данных ACCESS;</li> <li>– осуществлять ввод, редактирование и оформление информации;</li> <li>– работать с программами по архивации данных;</li> <li>– проверять файлы, диски и папки на наличие вирусов;</li> <li>– использовать средства защиты информации от несанкционированного доступа и случайных воздействий;</li> <li>– владеть правовыми аспектами информационной деятельности;</li> <li>– соблюдать санитарно-гигиенические требования, нормы и</li> </ul>

	<p>правила по охране труда.</p> <p>В результате освоения профессионального модуля обучающийся должен <b>узнать</b>:</p> <ul style="list-style-type: none"> <li>– архитектуру ЭВМ;</li> <li>– устройство системного блока и его основных узлов;</li> <li>– приемы ввода-вывода информации в ЭВМ;</li> <li>– правила включения, перезагрузки и выключения компьютера и периферийных устройств;</li> <li>– правила поиска и устранения сбоев в работе программ ЭВМ;</li> <li>– функции и группы клавиш на клавиатуре персонального компьютера, варианты клавиатурных комбинаций. Слепой метод набора текста;</li> <li>– структуру, свойства и возможности операционной системы Windows;</li> <li>– правила пользования текстовым редактором Word;</li> <li>– правила пользования электронными таблицами Excel;</li> <li>– правила пользования базами данных Access;</li> <li>– правила архивации и разархивации файлов;</li> <li>– разновидности антивирусных программ, принципы их действия, способы настройки и порядок работы с ними;</li> <li>– правовые аспекты информационной деятельности;</li> <li>– санитарно-гигиенические требования к организации рабочего места;</li> <li>– правила техники безопасности и противопожарной защиты.</li> </ul>
--	---

### **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:

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

	<p>расследования.</p> <p>ПК 2.9. Использовать нормативные правовые акты, нормативно-методические документы по защите информации.</p>
<p>ПМ.03 Программно-аппаратные и технические средства информации</p>	<p>ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.</p> <p>ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.</p> <p>ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.</p> <p>ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.</p>
<p>ПМ.04 Выполнение по одной или нескольким профессиям рабочих ,должностям служащих</p>	<p>ПК 4.1. Участвовать в разработке организационной структуры комплексной системы защиты информации (далее - КСЗИ).</p> <p>ПК 4.2. Участвовать в оценке технико-экономического уровня и эффективности организации КСЗИ.</p> <p>ПК 4.3. участвовать в подготовке заданий на реализацию КСЗИ.</p> <p>ПК 4.4. Организовывать и планировать работу малых коллективов исполнителей.</p>

Количество часов , отводимое на учебную практику

Всего: 4 неделя, 144 часов