# РЕЦЕНЗИЯ

на рабочую программу профессионального модуля
ПМ.04 Выполнение работ по одной или нескольким профессиям для специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем,
разработанную преподавателем Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет»
Катриковой Ц.Ю.

Представленная рабочая программа профессионального модуля ПМ.04 Выполнение работ по одной или нескольким профессиям разработана в соответствии с требованиями Федерального государственного образовательного стандарта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Структура рабочей программы соответствует структуре примерных программ профессиональных модулей среднего профессионального образования.

Рецензируемая рабочая программа профессионального модуля имеет чёткую структуру и включает все необходимые компоненты.

В общей характеристике рабочей программы раскрываются цели и задачи сформулированы цели и планируемые результаты освоения профессионального модуля.

Объем профессионального модуля, виды учебной работы, тематический план и содержание профессионального модуля раскрывают структуру и содержание профессионального модуля. Указанные объем часов обязательной аудиторной учебной нагрузки, практических занятий обучающихся и форма промежуточной аттестации соответствуют учебному плану.

В тематическом плане и содержании профессионального модуля раскрывается последовательность изучения разделов и тем программы, показываются распределение учебных часов по разделам, темам. Дидактические единицы, отраженные в содержании учебного материала, направлены на качественное усвоение учебного материала. Для приобретения практических навыков и повышения уровня знаний предусмотрены практические занятия.

Условия реализации профессионального модуля определяют требования к необходимому материально-техническому обеспечению к оборудованию учебной лаборатории и техническим средствам обучения.

Информационное обеспечение обучения содержит современный перечень основных печатных источников, дополнительных печатных источников и электронных источников.

Контроль и оценка результатов освоения профессионального модуля содержит код и наименование профессиональных и общих компетенций, критерии оценки, и методы оценки результатов обучения, которые осуществляются преподавателем в процессе проведения различных форм учебных занятий.

Рецензируемая рабочая программа рекомендуется для реализации в образовательном процессе.

Рецензент _____ Лиджи-Гаряев Б.Б., преподаватель Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно--экономический университет»

ОДОБРЕНА
Предметно-цикловой комиссией
естественнонаучных и
математических дисциплин

Разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

протокол № 1

от « 26 » 08 2021 г.

председатель предметно-цикловой комиссии
Катрикова Ц.Ю. /

заместитель директора по учебно-методической работе
Новгородова В.В. /

Составитель:

Катрикова Ц.Ю. , высшая квалификационная категория, преподаватель Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет»

Рецензенты:

Лиджи-Гаряев Б.Б., первая квалификационная категория, преподаватель Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет»

Агеев С.С., заместитель начальника отдела обеспечения деятельности, противодействия коррупции, кадров и защиты информации, министерства финансов Республики Калмыкия

# РЕЦЕНЗИЯ

на рабочую программу по производственной (преддипломной) практике для специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем, разработанную преподавателем Калмыцкого филиала ФГБОУИ ВО МГГЭУ Катриковой Ц.Ю.

Представленная рабочая программа по производственной (преддипломной) практике разработана с учетом требований Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Структура рабочей программы соответствует структуре примерных программ профессиональных модулей среднего профессионального образования.

В общей характеристике рабочей программы сформулированы цели и планируемые результаты освоения производственной практики (преддипломная), виды работ, обеспечивающих формирование профессиональных компетенций, количество часов, коды формируемых компетенций.

Объем производственной практики (преддипломная) и виды работ, предусмотренные ФГОС СПО и учебным планом по специальности, соответствуют тематическому содержанию производственной практики (преддипломная).

Содержание программы направлено на приобретение обучающимися знаний, умений, общих и профессиональных компетенций, определенных ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и соответствует объему часов, указанному в рабочем учебном плане.

Информационное обеспечение обучения содержит современный перечень основных печатных источников, дополнительных печатных источников и электронных источников.

Контроль и оценка результатов освоения производственной практики (преддипломная) осуществляется путем выполнения заданий на практике, подготовки дневника и контролируется руководителем производственной практики (преддипломной) от филиала и руководителем практики от организации (учреждения).

Рабочая программа позволит студентам в достаточной мере освоить виды работ, овладеть общими и профессиональными компетенциями, необходимых для качественного освоения программы подготовки специалистов среднего звена.

Рабочая программа производственной практики (преддипломной) рекомендуется к применению в учебном процессе Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно¬-экономический университет».

Рецензент _____ Агеев С.С., заместитель начальника отдела обеспечения деятельности, противодействия коррупции кадров и защиты информации, Министерства финансов Республики Калмыкия

РЕЦЕНЗИЯ

на рабочую программу по производственной (преддипломной) практики для специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем, разработанную преподавателем Калмыцкого филиала ФГБОУИ ВО МГГЭУ Катриковой Ц.Ю.

Представленная рабочая программа производственной (преддипломной) практики разработана с учетом требований Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Структура рабочей программы соответствует структуре примерных программ профессиональных модулей среднего профессионального образования.

В общей характеристике рабочей программы сформулированы цели и планируемые результаты освоения производственной практики (**преддипломная**), виды работ, обеспечивающих формирование профессиональных компетенций, количество часов, коды формируемых компетенций.

Объем производственной практики (**преддипломная**) и виды работ, предусмотренные ФГОС СПО и учебным планом по специальности, соответствуют тематическому содержанию производственной практики (**преддипломная**).

Содержание программы направлено на приобретение обучающимися знаний, умений, общих и профессиональных компетенций, определенных ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и соответствует объему часов, указанному в рабочем учебном плане.

Информационное обеспечение обучения содержит современный перечень основных печатных источников, дополнительных печатных источников и электронных источников.

Контроль и оценка результатов освоения производственной практики (**преддипломная**) осуществляется путем выполнения заданий на практике, подготовки дневника и контролируется руководителем производственной практики (преддипломной) от филиала и руководителем практики от организации (учреждения).

Рабочая программа позволит студентам в достаточной мере освоить виды работ, овладеть общими и профессиональными компетенциями, необходимых для качественного освоения программы подготовки специалистов среднего звена.

Рабочая программа производственной практики (преддипломной) рекомендуется к применению в учебном процессе Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет».

Рецензент _____ Лиджи-Гаряев Б.Б., преподаватель Калмыцкого филиала ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет»

СОДЕРЖАНИЕ

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

1.1. Цель и планируемые результаты освоения производственной практики (преддипломной)

1.1.1. В результате изучения профессионального модуля студент должен освоить основные виды деятельности: эксплуатация автоматизированных (информационных) систем в защищенном исполнении; защита информации в автоматизированных системах программными и программно-аппаратными средствами; защита информации техническими средствами

| Код | Наименование видов деятельности и профессиональных компетенций |
|---|---|
| ВД 1 | Эксплуатация автоматизированных (информационных) систем в защищенном исполнении |
| ВД 2 | Защита информации в автоматизированных системах программными и программно-аппаратными средствами |
| ВД 3 | Защита информации техническими средствами |
| ПК 1.1. | Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации. |
| ПК 1.2. | Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении. |
| ПК 1.3. | Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации. |
| ПК 1.4. | Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении. |
| ПК 2.1. | Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. |
| ПК 2.2. | Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. |
| ПК 2.3. | Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. |
| ПК 2.4. | Осуществлять обработку, хранение и передачу информации ограниченного доступа. |
| ПК 2.5. | Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. |
| ПК 2.6. | Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. |
| ПК 3.1. | Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации. |
| ПК 3.2. | Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации. |
| ПК 3.3. | Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки |

| | |
|---|---|
| | информации ограниченного доступа. |
| ПК 3.4. | Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. |
| ПК 3.5. | Организовывать отдельные работы по физической защите объектов информатизации. |

1.1.2. Общие компетенции:

| Код | Наименование видов деятельности и профессиональных компетенций |
|---|---|
| ОК 1. | Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. |
| ОК 2. | Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. |
| ОК 3. | Планировать и реализовывать собственное профессиональное и личностное развитие. |
| ОК 4. | Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. |
| ОК 5. | Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. |
| ОК 6. | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения. |
| ОК 7. | Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. |
| ОК 8. | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности. |
| ОК 9. | Использовать информационные технологии в профессиональной деятельности. |
| ОК 10. | Пользоваться профессиональной документацией на государственном и иностранном языках. |
| ОК 11. | Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере. |

1.1.3. В результате освоения профессионального модуля студент должен:

| | |
|---|---|
| Иметь практический опыт | – установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем в защищённом исполнении;<br>– администрирования автоматизированных систем в защищенном исполнении;<br>– эксплуатации компонентов систем защиты информации автоматизированных систем;<br>диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении<br>– установки, настройки программных средств защиты информации в автоматизированной системе;<br>– обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;<br>– тестирования функций, диагностика, устранения отказов и |

| | |
|---|---|
| | восстановления работоспособности программных и программно-аппаратных средств защиты информации ;<br>– решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;<br>– применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;<br>– учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;<br>– работы с подсистемами регистрации событий;<br>выявления событий и инцидентов безопасности в автоматизированной системе.<br>– установки, монтажа и настройки технических средств защиты информации;<br>– технического обслуживания технических средств защиты информации;<br>– применения основных типов технических средств защиты информации;<br>– выявления технических каналов утечки информации;<br>– участия в мониторинге эффективности технических средств защиты информации;<br>– диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;<br>– проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;<br>– проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;<br>установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты. |
| уметь | – осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем;<br>– организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;<br>– осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;<br>– производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;<br>– настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам;<br>обеспечивать работоспособность, обнаруживать и устранять неисправности |

| | |
|---|---|
| | – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;<br>– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;<br>– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;<br>– применять программные и программно-аппаратные средства для защиты информации в базах данных;<br>– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;<br>– применять математический аппарат для выполнения криптографических преобразований;<br>– использовать типовые программные криптографические средства, в том числе электронную подпись;<br>– применять средства гарантированного уничтожения информации;<br>– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;<br>– осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак<br>– применять технические средства для криптографической защиты информации конфиденциального характера;<br>– применять технические средства для уничтожения информации и носителей информации;<br>– применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;<br>– применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;<br>– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;<br>применять инженерно-технические средства физической защиты объектов информатизации |
| знать | – состав и принципы работы автоматизированных систем, операционных систем и сред;<br>– принципы разработки алгоритмов программ, основных приемов программирования;<br>– модели баз данных;<br>– принципы построения, физические основы работы периферийных устройств;<br>– теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;<br>–порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях;<br>–принципы основных методов организации и проведения технического |

| | |
|---|---|
| | обслуживания вычислительной техники и других технических средств информатизации.<br>– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;<br>– методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;<br>– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;<br>– основные понятия криптографии и типовых криптографических методов и средств защиты информации;<br>– особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;<br>типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.<br>– порядок технического обслуживания технических средств защиты информации;<br>– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;<br>– физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;<br>– порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;<br>– методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;<br>– номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;<br>– основные принципы действия и характеристики технических средств физической защиты;<br>– основные способы физической защиты объектов информатизации;<br>номенклатуру применяемых средств физической защиты объектов информатизации. |

1.2. Цель и задачи производственной практики (по профилю специальности) по профессиональному модулю 04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

Целями производственной практики (преддипломной) являются:

- сбор материала, необходимого для выполнения выпускной квалификационной работы в соответствии с избранной темой и планом, согласованным с руководителем выпускной квалификационной работы;
- углубление и закрепление теоретических знаний в соответствии с

обозначенными образовательным стандартом общими и профессиональными компетенциями, подготовка к самостоятельной работе по специальности.

Задачами производственной практики (преддипломной) являются:

- приобретение глубоких профессиональных навыков, необходимых при решении конкретных профессиональных задач в определенном виде деятельности, установленном ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем;
- сбор, обобщение и анализ практического материала, необходимого для подготовки и написания выпускной квалификационной работы;
- анализ деятельности конкретного предприятия в области информатизации процессов;
- развитие навыков профессиональной рефлексии;
- овладение современными методами сбора, анализа и обработки научной информации по проблеме;
- подбор и анализ основных и дополнительных источников и литературы в соответствии с проблематикой выпускной квалификационной работы, выполняемых в период производственной практики (преддипломной).

1.3. Рекомендуемое количество часов на освоение рабочей программы производственной практики (преддипломной)

Бюджет времени на производственную практику (преддипломную) для получения профессиональных умений и навыков определен в объеме 144 часа.

## 2. СТРУКТУРА И СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

### 2.1. Тематический план и содержание производственной практики (преддипломной)

| № | Наименование темы | Количество дней |
|---|---|---|
| 1. | Характеристика базы производственной практики (преддипломной) (органа социального обеспечения граждан). | 1 |
| 2. | Подбор нормативно-правовых актов, учебной и научной литературы, электронных ресурсов. | 1 |
| 3. | Написание введения выпускной квалификационной работы | 1 |
| 4. | Формирование материалов главы 1 выпускной квалификационной работы на основе анализа нормативных актов базы производственной практики (преддипломной) | 2 |
| 5. | Формирование материалов главы 2 выпускной квалификационной работы на основе анализа нормативных актов б&зы производственной практики (преддипломной) | 2 |
| 6. | Формирование материалов главы 3 выпускной квалификационной работы с учетом данных базы производственной практики (преддипломной) | 14 |
| 7. | Написание заключения и оформление выводов по выпускной квалификационной работе | 1 |
| 8. | Систематизация списка использованных источников и литературы и формирование приложений выпускной квалификационной работы | 1 |
| 9 | Формирование отчета производственной практики (преддипломной) | 1 |
| | Итого | 24 |

## 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРОЕДДИПЛОМНОЙ)

3.1. Требования к документации, необходимой для проведения производственной практики (преддипломной)

1. Договор с организацией (учреждением) о проведении производственной практики (преддипломной);
2. Приказ о распределении обучающихся по местам производственной практики (преддипломной) и назначение руководителя производственной практики (преддипломной) от учебного заведения;
3. Рабочая программа производственной практики (преддипломной);
4. Тематический план и содержание производственной практики (преддипломной);
5. Дневник прохождения производственной практики (преддипломной);
6. Аттестационный лист и характеристика от организации (учреждения).

3.2. Требования к учебно-методическому обеспечению производственной практики (преддипломной)

Производственная практика (преддипломная) направлена на формирование у обучающихся общих и профессиональных компетенций, приобретение практического опыта по каждому из видов профессиональной деятельности, предусмотренных ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

- Наличие учебно-методического обеспечения производственной практики (преддипломной):
- Рабочая программа производственной практики (преддипломной);
- Тематический план и содержание производственной практики (преддипломной);
- Дневник о прохождении производственной практики (преддипломной);
- Аттестационный лист и характеристика от организации (учреждения).

3.3. Требования к материально-техническому обеспечению производственной практики (преддипломной)

Производственная практика (преддипломная) должна проводиться в организациях (учреждениях), направление деятельности которых соответствует профилю подготовки обучающихся и с соответствующим материально-техническим обеспечением.

3.4. Информационное обеспечение обучения

3.4.1. Основные печатные источники:

1. В.П. Мельников, А.И. Куприянов Информационная безопасность : учебник / В.П. Мельников, А.И. Куприянов ; под ред. В.П. Мельникова. - 2-е изд., перераб. и доп. - Москва : КНОРУС, 2018. - 268 с. - (Среднее профессиональное образование). ISBN 978-5-406-05072-92.

2. Матвеев Р.Ф. Правовое обеспечение профессиональной деятельности: учебное пособие для среднего профессионального образования / Р.Ф.Матвеев. - М.: КНОРУС, 2018,- 158 с.
3. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. - Москва : Издательство Юрайт, 2018. - 342 с. - (Профессиональное образование). - ISBN 978-5-534-10671-8.
4. Зайцев А.П. Технические средства и методы защиты информации: Учебник для СПО / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. - М.: ООО «Издательство Машиностроение», 2018 - 508 с. ISBN 978-5-94275-454-9

3.4.2. Дополнительные печатные источники:

1. Компьютерные сети и телекоммуникации. Маршрутизация в ip-сетях в 2 ч. Часть 1 : учебник и практикум для СПО / М. В. Дибров. — М. : Юрайт, 2017 — 351 с. — (Серия : Профессиональное образование). — ISBN 978-5-53404635-9. — Режим доступа : www.biblio-online.ru/book/9C59BC84-8E5B-488E- 94CB-8725668917BD
2. Компьютерные сети и телекоммуникации. Маршрутизация в ip-сетях в 2 ч. Часть 2 : учебник и практикум для СПО / М. В. Дибров. — М. : Юрайт, 2017 — 351 с. — (Серия : Профессиональное образование). — ISBN 978-5-53404635-9. — Режим доступа : www.biblio-online.ru/book/9C59BC84-8E5B-488E- 94CB-8725668917BD.
3. Криптографические методы защиты информации : учебник для
4. академического бакалавриата / С. В. Запечников, О. В.иКазарин, А. А. Тарасов.
5. М. : Юрайт, 2017 — 309 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-02574-3. — Режим доступа: www.biblio-
6. online.ru/book/B27D8A2B-F86C-4F 18-9F21 - 3E0695C0A4C0.
7. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
8. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
9. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
10. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
11. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
12. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
13. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации

при использовании информационно-телекоммуникационных сетей международного информационного обмена».
14. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
15. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
16. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
17. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
18. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
19. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
20. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
21. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
22. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
23. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
24. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
25. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня
26. 2001 г.
27. № 152 «Об утверждении инструкции об организации и обеспечении
28. безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с
29. ограниченным доступом, не содержащей сведений, составляющих

30. государственную тайну».
31. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении
32. Положения о разработке, производстве, реализации и эксплуатации
33. шифровальных (криптографических) средств защиты информации».
34. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология.
35. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных
36. технологий
37. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
38. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
39. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
40. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
41. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
42. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
43. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
44. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
45. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
46. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.
47. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
48. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

49. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкоссией России, 20ми02.
50. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
51. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
52. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

3.4.3. Электронные источники:

1. http://wm-help.net/books-online/book/98618/98618-7.html - принципы защиты операционных систем
2. http://rudocs.exdat.com/docs/index-56877.html - принципы построения операционных систем
3. http://www.winblog.ru/2006/08/21/21080608.html - система парольной защиты
4. http://emanual.ru/download/6661.html - средства безопасности для защиты сервисов
5. http://www.supermegayo.rU/vlomprogr/3.html - Атаки на программное обеспечение.

3.5. Обязанности обучающегося в период производственной практики (преддипломной)

- Изучить программу прохождения производственной практики (преддипломной), подготовить соответствующие программные материалы.
- Своевременно прибывать на базу производственной практики (преддипломной), имея при себе все необходимые документы: программу производственной практики (преддипломной), дневник о прохождении производственной практики (преддипломной).
- Строго выполнять действующие в организации (учреждении) правила внутреннего распорядка, не допускать нарушения трудовой дисциплины. Добросовестно выполнять все указания руководителя производственной практики (преддипломной) от организации (учреждении), касающиеся порядка прохождения и содержания производственной практики (преддипломной), индивидуальные поручения руководителя практики от организации (учреждении), активно участвовать во всех мероприятиях, к которым обучающийся привлекается.'
- Подготовить дневник о прохождении производственной практики (преддипломной) в соответствии с установленными данной программой требованиями, подписать его, а также заверить у руководителя производственной практики (преддипломной) от организации (учреждении).

3.3. Особенности обучения инвалидов и лиц с ограниченными возможностями здоровья

Учебные занятия инвалидов и лиц с ограниченными возможностями здоровья организуются совместно с другими обучающимися в учебных группах, а также индивидуально, в соответствии с графиком индивидуальных занятий.

При этом необходимо учитывать несколько аспектов:

- особенности нозологии обучающихся инвалидов и лиц с ограниченными возможностями здоровья;
- психоэмоциональное состояния обучающихся;
- психологический климат, который сложился в студенческой группе;
- настрой отдельных обучающихся и группы в целом на процесс обучения.

При организации учебных занятий в учебных группах используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений, создания комфортного психологического климата в группе.

В образовательной деятельности применяются материально-техническое оснащение, специализированные технические средства приема-передачи учебной информации в доступных формах для обучающихся с различными особенностями здоровья, электронные образовательные ресурсы в адаптированных формах.

Специфика обучения инвалидов и обучающихся с ограниченными возможностями здоровья предполагает использование игрового, практико-ориентированного, занимательного материала, который необходим для получения знаний и формирования необходимых компетенций. Подготовка обучающимися заданий для учебных занятий должна сочетать устные и письменные формы в соответствии с их особенностями здоровья.

Для того чтобы предотвращать наступление у обучающихся с инвалидностью и обучающихся, имеющих ограниченные возможности здоровья, быстрого утомления можно использовать следующие методы работы:

- чередование умственной и практической деятельности;
- преподнесение материала с использованием средств наглядности;
- использование технических средств обучения, чередование предъявляемой на слух информации с наглядно-демонстрационным материалом.

При освоении дисциплин инвалидами и лицами с ограниченными возможностями здоровья большое значение должно отводиться проведению с ними индивидуальной работы со стороны преподавателей. В индивидуальную работу включается:

- индивидуальная учебная работа (консультации), то есть дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы;

- индивидуальная воспитательная работа.

Особенности обучения обучающихся с нарушениями опорно-двигательного аппарата.

Для обучающегося, имеющего нарушения опорно-двигательного аппарата, необходимо посоветовать использовать вспомогательные средства для усвоения программы, например, диктофон и другие электронные носители информации.

При проведении аудиторных занятий с обучающимися, имеющими осложнения с моторикой рук, возможно использование следующих вариантов работы:

- обеспечение обучающихся электронными текстами лекций и заданий к учебным занятиям;

- использование технических средств фиксации текста (диктофоны) с последующим составлением тезисов лекции в ходе самостоятельной работы обучающегося, которые они впоследствии могут использовать при подготовке и ответах на учебных занятиях.

Одним из видов работы для обучающихся, испытывающих трудности в письме может быть подготовка к учебным занятиям таких заданий, которые не требуют от них написания длинных текстов ответов. Наиболее оптимальным вариантом такого задания, выполняемого в письменной форме, может служить тестовое задание. Использование тестирования обучающихся необходимо совмещать с обсуждением вариантов ответов.

Контроль знаний можно вести как в устном, так и в письменном виде.

Особенности обучения обучающихся с нарушением слуха.

При организации образовательного процесса со слабослышащей аудиторией рекомендуется использовать следующие педагогические принципы:

- наглядности преподаваемого материала;

- индивидуального подхода к каждому обучающемуся;

- использования информационных технологий;

- использования учебных пособий, адаптированных для восприятия обучающимися с нарушением слуха.

Обучающемуся с нарушением слуха следует предложить занять место на передних партах аудитории, а преподавателю больше времени находиться рядом с рабочим местом этого обучающегося. Учитывая, что такие обучающиеся лучше понимают по губам, желательно располагаться к ним лицом, говорить громко и четко.

Для повышения уровня восприятия учебной информации обучающимися рассматриваемой группы, рекомендуется применение звукоусиливающей аппаратуры, мультимедийных и других средств. Сложные для понимания темы следует снабжать как можно большим количеством наглядного материала. Особую роль в обучении лиц с нарушенным слухом, играют видеоматериалы. По возможности, предъявляемая видеоинформация может сопровождаться текстовой бегущей строкой или сурдологическим переводом.

Контроль знаний обучающихся указанной нозологии может вестись преимущественно в письменном виде, но для развития устной речи, рекомендуется предложить обучающемуся рассказать ответ на задание в тезисах.

Особенности обучения обучающихся с нарушением зрения.

Специфика обучения слабовидящих обучающихся заключается в следующем:

- необходимо дозировать учебную нагрузку;

- применять специальные формы и методы обучения, технические средства, позволяющие воспринимать информацию, а также оптические и тифлопедагогические устройства, расширяющие познавательные возможности обучающихся;

- увеличивать искусственную освещенность помещений, в которых занимаются обучающиеся с пониженным зрением.

При зрительной работе у слабовидящих обучающихся быстро наступает утомление, что снижает их работоспособность, поэтому необходимо проводить небольшие перерывы или переключение рабочей активности.

При чтении лекций, слабовидящим обучающимся следует разрешить использовать звукозаписывающие устройства и компьютеры, как способ конспектирования, во время занятий. Необходимо комментировать свои жесты и надписи на доске и передавать словами то, что часто выражается мимикой и жестами.

При работе на компьютере следует использовать принцип максимального снижения зрительных нагрузок, дозирование и чередование зрительных нагрузок с другими видами деятельности. Кроме того необходимо использовать специальные программные средства для увеличения изображения на экране или для озвучивания информации.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

1. информация по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, на электронном носителе, в печатной форме увеличенным шрифтом и т.п.);

2. доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа);

3. доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, устно и др.).

При необходимости для обучающихся с инвалидностью и обучающихся с ограниченными возможностями здоровья процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов, а также может быть предоставлено дополнительное время для подготовки ответа на зачете или экзамене.

# 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

Выполнение заданий на практике, подготовка дневника, характеристики и аттестационного листа контролируется руководителем производственной практики (преддипломной) от филиала и руководителем практики от организации (учреждения). Сдача и защита дневника о прохождении производственной практики (преддипломной) проводится в последний день проведения данной практики.

Структура дневника о прохождении производственной практики (преддипломной) включает:

1. Титульный лист (Приложение 1);
2. Тематический план и содержание производственной практики (преддипломной) (Приложение 2);
3. Дневник прохождения производственной практики (преддипломной) (Приложение 3);
4. Аттестационный лист (Приложение 4) с указанием сформированных в период производственной практики (преддипломной) общих компетенций и приобретения практического опыта (Приложение 5) и характеристика от руководителя практики от организации (учреждения) о работе обучающегося;
5. Задание на выполнение выпускной квалификационной работы;
7. Сформированный список использованных источников и литературы;
8. Приложения (макет пенсионного или социального дела).

Обучающийся, не выполнивший без уважительной причины программы производственной практики (преддипломной), отчисляется из учебного заведения как имеющий академическую задолженность. В случае уважительной причины студент направляется на практику вторично, а государственная (итоговая) аттестация переносится на следующий учебный год.

Приложение 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ

**«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»**

КАЛМЫЦКИЙ ФИЛИАЛ

# ДНЕВНИК - ОТЧЕТ
# О ПРОХОЖДЕНИИ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ
# (ПРЕДДИПЛОМНОЙ)

на _____
(наименование предприятия)

с _____по _____ 20_____г.
(срок прохождения практики)

Студента гр._____ _ _____

Руководитель практики от организации _____

Руководитель практики от филиала _____

Оценка

Элиста 20__г

Приложение 2

ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

| № | Наименование темы | Количество дней | | Сроки выполнения | |
|---|---|---|---|---|---|
| | | План | Факт | План | Факт |
| 1. | Характеристика базы производственной практики (преддипломной) (органа социального обеспечения граждан). | 1 | 1 | | |
| 2. | Подбор нормативно-правовых актов, учебной и научной литературы, электронных ресурсов. | 1 | 1 | | |
| 3. | Написание введения выпускной квалификационной работы | 1 | 1 | | |
| 4. | Формирование материалов главы 1 выпускной квалификационной работы на основе анализа нормативных актов базы производственной практики (преддипломной) | 2 | 2 | | |
| 5. | Формирование материалов главы 2 выпускной квалификационной работы на основе анализа нормативных актов базы производственной практики (преддипломной) | 2 | 2 | | |
| 6. | Формирование материалов главы 3 выпускной квалификационной работы с учетом данных базы производственной практики (преддипломной) | 14 | 14 | | |
| 7. | Написание заключения и оформление выводов по выпускной квалификационной работе | 1 | 1 | | |
| 8. | Систематизация списка использованных источников и литературы и формирование приложений выпускной квалификационной работы | 1 | 1 | | |
| 9 | Формирование отчета производственной практики (преддипломной) | 1 | 1 | | |
| | Итого | 24 | 24 | | |

Руководитель практики от филиала _____

М.П.

Приложение 3

ДНЕВНИК ПРОХОЖДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ
(ПРЕДДИПЛОМНОЙ)

| Дата | Содержание работ | Подпись руководителя практики от филиала |
|---|---|---|
| | | |

ПРИЛОЖЕНИЕ 4

АТТЕСТАЦИОННЫЙ ЛИСТ
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)
(заключение руководителя практики от организации (учреждения))

1. ФИО студента, № группы, специальность_____
_____

2. Место проведения производственной практики (преддипломной) наименование организации
(учреждения) _____

3. Время проведения практики _____

4. Виды и объем работ, выполненные студентом во время практики:

| № | Наименование темы | Количество дней |
|---|---|---|
| 1. | Характеристика базы производственной практики (преддипломной) (органа социального обеспечения граждан) | 1 |
| 2. | Подбор нормативно-правовых актов, учебной и научной литературы, электронных ресурсов | 1 |
| 3. | Написание введения выпускной квалификационной работы | 1 |
| 4. | Формирование материалов главы 1 выпускной квалификационной работы на основе анализа нормативных актов базы производственной практики (преддипломной) | 2 |
| 5. | Формирование материалов главы 2 выпускной квалификационной работы на основе анализа нормативных актов базы производственной практики (преддипломной) | 2 |
| 6. | Формирование материалов главы 3 выпускной квалификационной работы с учетом данных базы производственной практики (преддипломной) | 14 |
| 7. | Написание заключения и оформление выводов по выпускной квалификационной работе | 1 |
| 8. | Систематизация списка использованных источников и литературы и формирование приложений выпускной квалификационной работы | 1 |
| 9 | Формирование отчета производственной практики (преддипломной) | 1 |
| | Итого | 24 |

5. Качество выполнения работ в соответствии с технологией и (или) требованиями организации, в которой проходила практика
_____
_____
_____
_____

Руководитель практики от организации (учреждения) _____ / _____ /
подпись ФИО

МП

Руководитель практики от филиала _____ / _____ /
подпись ФИО

Приложение 5

# РЕКОМЕНДАЦИИ
## по оформлению аттестационного листа производственной практики (преддипломной)

1. Виды и объем работ, выполненные студентом во время практики – перечень отработанных тем и вопросов согласно программы производственной практики.

2. Качество выполнения работ в соответствии с технологией и (или) требованиями организации, в которой проходила практика. Указать какими общими и профессиональными компетенциями обладает выпускник по результатам прохождения производственной практики.

Студент специальности 10.02.05 Обеспечение информационнойбезопасности автоматизированных систем должен обладать общими и профессиональными компетенциями, включающими в себя способность:

| **Код и формулировка компетенции** | **Показатели освоения компетенции** |
|---|---|
| ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам | **Умения:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы;<br>владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника). |
| | **Знания:** актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте, алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности. |

| | |
|---|---|
| ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности | **Умения:** определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска. |
| | **Знания** номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации |
| ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие | **Умения:** определять актуальность нормативноправовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития |
| | **Знания:** содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования |
| ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами | **Умения:** организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами |
| | **Знания:** психология коллектива; психология личности; основы проектной деятельности |
| ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста | **Умения:** излагать свои мысли на государственном языке; оформлять документы. |
| | **Знания:** особенности социального и культурного контекста; правила оформления документов. |
| ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей | **Умения:** описывать значимость своей профессии<br>Презентовать структуру профессиональной деятельности по специальности |
| | **Знания:** сущность гражданско-патриотической позиции<br>Общечеловеческие ценности<br>Правила поведения в ходе выполнения профессиональной деятельности |
| ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях | **Умения:** соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности. |
| | **Знания:** правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения. |

| | |
|---|---|
| ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности | **Умения:** использовать физкультурнооздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности |
| | **Знания:** роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения. |
| ОК 9. Использовать информационные технологии в профессиональной деятельности | **Умения:** применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение |
| | **Знания:** современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности. |
| ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках | **Умения:** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы |
| | **Знания:** правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности |
| ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации | **Практический опыт:** установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем |
| | **Умения:** осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем |
| | **Знания**: состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, |

| | |
|---|---|
| | основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств |
| ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении | **Практический опыт:** администрирование автоматизированных систем в защищенном исполнении |
| | **Умения:** организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;<br>производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы |
| | **Знания:** теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации |
| ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации | **Практический опыт:** эксплуатация компонентов систем защиты информации автоматизированных систем |
| | **Умения:** настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам |
| | **Знания:** порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях |
| ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении | **Практический опыт:** диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении |
| | **Умения:** обеспечивать работоспособность, обнаруживать и устранять неисправности |
| | **Знания:** принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации |
| ПК 2.1. Осуществлять установку и настройку отдельных программных, программноаппаратных средств защиты информации | **Практический опыт:** установка, настройка программных средств защиты информации в автоматизированной системе |
| | **Умения:** устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; |
| | **Знания:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных |
| ПК 2.2. Обеспечивать защиту информации в автоматизированных системах | **Практический опыт:** обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; |

| | |
|---|---|
| отдельными программными, программно-аппаратными средствами. | использование программных и программноаппаратных средств для защиты информации в сети |
| | **Умения:** устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;<br>устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; |
| | **Знания:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных |
| ПК 2.3. Осуществлять тестирование функций отдельных программных и программноаппаратных средств защиты информации | **Практический опыт:** тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программноаппаратных средств защиты информации |
| | **Умения:** диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; |
| | **Знания:** методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации |
| ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа | **Практический опыт:** решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;<br>применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных<br>использовать типовые программные криптографические средства, в том числе электронную подпись |
| | **Знания:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;<br>основные понятия криптографии и типовых криптографических методов и средств защиты информации |
| ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств | **Практический опыт:** учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности |
| | **Умения:** применять средства гарантированного уничтожения информации |
| | **Знания:** особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации |
| ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в | **Практический опыт:** работа с подсистемами регистрации событий;<br>выявление событий и инцидентов безопасности в автоматизированной системе |

| | |
|---|---|
| том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак | **Умения:** устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;<br>осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак |
| | **Знания:** типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа |
| ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации | **Практический опыт:** установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации;<br>применение основных типов технических средств защиты информации |
| | **Умения:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных |
| | **Знания:** порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам |
| ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации | **Практический опыт:** применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации;<br>диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации |
| | **Умения:** применять технические средства для криптографической защиты информации конфиденциального характера;<br>применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами |
| | **Знания:** физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;<br>порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, |

| | |
|---|---|
| | обрабатываемой средствами вычислительной техники на объектах информатизации;<br>номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам |
| ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа | **Практический опыт:** проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации |
| | **Умения:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных |
| | **Знания:** номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;<br>структуру и условия формирования технических каналов утечки информации; |
| ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации | **Практический опыт:** проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;<br>выявление технических каналов утечки информации |
| | **Умения:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных |
| | **Знания:** номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам |
| ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации | **Практический опыт:** установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженернотехнических средств физической защиты |
| | **Умения:** применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;<br>применять инженерно-технические средства физической защиты объектов информатизации |
| | **Знания:** основные принципы действия и характеристики технических средств физической защиты;<br>основные способы физической защиты объектов информатизации;<br>номенклатуру применяемых средств физической защиты объектов информатизации |