



Автономная некоммерческая профессиональная образовательная организация
«Многопрофильная Академия непрерывного образования»
АНПОО «МАНО»
Колледж

ПРИНЯТО

Решением Педагогического совета

АНПОО «МАНО»

Протокол № 01-01/16 от

01.06.2022 г.

УТВЕРЖДАЮ

Директор АНПОО «МАНО»



В.И. Гам

июня 20 22 г.

РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА

УЧЕБНОЙ ПРАКТИКИ

по профессиональному модулю

**ПМ.1 «УЧАСТИЕ В ПЛАНИРОВАНИИ И ОРГАНИЗАЦИИ РАБОТ ПО
ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ОБЪЕКТА»**

для специальности

10.02.01 Организация и технология защиты информации

Заочная форма обучения

Программа учебной практики профессионального модуля разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) **10.02.01 Организация и технология защиты информации.**

Организация-разработчик:

АНПОО «Многопрофильная Академия непрерывного образования».

Разработчик: Гам А.В., преподаватель.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	стр. 4
2. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРАКТИКИ	7
3. ФОРМЫ ОТЧЕТНОСТИ ПО ИТОГАМ ПРАКТИКИ	9
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ	10
5. ПЕРЕЧЕНЬ РЕКОМЕНДУЕМЫХ УЧЕБНЫХ ИЗДАНИЙ, ИНТЕРНЕТ-РЕСУРСОВ, ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ	14

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

ПМ. 1 Участие в планировании и организации работ по обеспечению защиты объекта

1.1. Место учебной практики в структуре основной профессиональной образовательной программы

Программа учебной практики является частью основной профессиональной образовательной программы (далее – ОПОП) по специальности СПО 10.02.01 Организация и технология защиты информации, в части освоения основного вида профессиональной деятельности: участие в планировании и организации работ по обеспечению защиты объекта.

1.2. Цель учебной практики

Целью учебной практики является освоение вида профессиональной деятельности «Участие в планировании и организации работ по обеспечению защиты объекта», закрепление и углубление знаний и умений, формирование общих и профессиональных компетенций, приобретение практического опыта в рамках профессионального модуля ПМ.01 «Участие в планировании и организации работ по обеспечению защиты объекта».

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

- использования физических средств защиты объекта;
- применения физических средств контроля доступа на объект;
- ведения текущей работы исполнителей с конфиденциальной информацией;

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;

знать:

- 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.

ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ПРОГРАММЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ СРЕДНЕГО ЗВЕНА:

5.1 Техник по защите информации должен обладать общими компетенциями, включающими в себя способность:

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

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

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

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

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ОК 10. Применять математический аппарат для решения профессиональных задач.

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

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

5.2. Техник по защите информации должен обладать профессиональными компетенциями, соответствующими видам деятельности:

5.2.1. 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.

1.3. Количество часов на освоение программы практики

Рабочая программа рассчитана на прохождение студентами практики в объеме 216 часов.

1.4. Требования к базам практики

Место и время проведения учебной практики

Практика проводится согласно календарному учебному графику, утвержденному директором колледжа. Практика обучающихся проводится в организациях на основе прямых договоров между колледжем и организацией, в которую направляются обучающиеся. Направление деятельности организаций должно соответствовать профилю подготовки обучающихся.

2. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРАКТИКИ

Наименование профессионального модуля, МДК, разделов	Содержание практики, виды работ, задания	Объем часов
ПМ 1 Участие в планировании и организации работ по обеспечению защиты объекта	<p>Ознакомление с предприятием и рабочими местами.</p> <ol style="list-style-type: none"> 1. Задачи и краткое содержание учебной практики по специальности. 2. Инструктаж по общим вопросам, охране труда и технике безопасности, по режиму работы предприятия. 3. Изучение структуры предприятия и взаимосвязи подразделений. Основная деятельность предприятия. <p>Обеспечение организации системы безопасности предприятия</p> <ol style="list-style-type: none"> 1. Организационно-штатная структура службы корпоративной безопасности. 2. Основные функциональные цели и задачи службы корпоративной безопасности. 3. Функциональные подразделения: их штатная структура. <p>Организация работ подразделений защиты информации</p> <ol style="list-style-type: none"> 1. Виды конфиденциальной информации организации. 2. Кадровая безопасность организации. <p>Организация работы персонала с конфиденциальной информацией</p> <ol style="list-style-type: none"> 1. Активный и пассивный доступ к информационным ресурсам. Проблемы, возникающие при реализации правовых мер защиты информации. 2. Система сбора и накопления информации. 3. Информационные базы. 4. Система переработки информации. 5. Система аналитической деятельности. 	216
Итоговая аттестация	Дифференцированный зачет	
		Всего: 216

	Задание
Учебная практика 3 семестр	<ol style="list-style-type: none"> 1. Виды и способы охраны объекта. 2. Особенности охраны персонала организации. 3. Основные направления и методы организации режима охраны объекта. 4. Каналы утечки информации. Технические средства обнаружения каналов утечки информации. Как определяется эффективность использования средств обнаружения возможных каналов утечки информации? Участие в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации. 5. Разрешительная система доступа к конфиденциальной информации. 6. Изложите обобщенную методику применения систем контроля доступа для организации защиты информации в организации. 7. Чем отличается методика выделения зоны доступа по типу конфиденциальности работ от степени конфиденциальности работ? На чем основана методика выделения зоны доступа по типу и степени конфиденциальности работ? 8. Принципы действия аппаратуры систем контроля доступа. 9. Принципы построения и функционирования биометрических систем безопасности. 10. Требования и особенности оборудования режимных помещений. 11. Методы проверки персонала по защите информации. 12. Процедура служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.
Учебная практика 5 семестр	<ol style="list-style-type: none"> 1. Техника безопасности при проведении организационно-технических мероприятий. 2. Требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров; 3. Требования режима защиты информации при приеме в организации посетителей; 4. Организация работы при осуществлении международного сотрудничества; 5. Требования режима защиты информации в процессе рекламной деятельности; 6. Требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати; 7. Задачи, функции и структура подразделений защиты информации; 8. Принципы, методы и технология управления подразделений защиты информации; 9. Критерии подбора и расстановки сотрудников подразделений защиты информации; 10. Организация работы с персоналом, имеющим доступ к конфиденциальной информации; 11. Инструктаж персонала по организации работы с конфиденциальной информацией; 12. Контроль за соблюдением персоналом требований режима защиты

	информации. 13. Оценка качества защиты объекта. 14. Осуществление планирования и организации выполнения мероприятий по защите информации.
--	---

3. ФОРМЫ ОТЧЕТНОСТИ ПО ИТОГАМ ПРАКТИКИ

- дневник практиканта,
- отчет студента о проделанной работе,
- характеристика руководителя практики от принимающей стороны.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Работа над отчетом по практике должна позволить руководителю оценить уровень развития следующих профессиональных и общих компетенций студента:

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 1.1. Участвовать в сборе и обработке материалов для выработки оптимальных решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.	<ul style="list-style-type: none"> - определение методов эффективного использования средств обнаружения возможных каналов утечки конфиденциальной информации; - выполнение анализа научной литературы; - обоснование выбора соответствующих решений по защите информации объекта; - обоснование использованных методов обнаружения технических каналов утечки информации 	Отчет по учебной практике
ПК 1.2. Участвовать в разработке программ и методик организации защиты информации на объекте	<ul style="list-style-type: none"> - определение предложений по разработке программ защиты информации на объекте; - определение методик защиты информации на предприятии 	
ПК 1.3. Осуществлять планирование и организацию выполнения мероприятий по защите информации	<ul style="list-style-type: none"> - выполнение работ по защите конфиденциальной информацией; - определение качества защиты информации; - выполнение мероприятий по комплексной защите информации 	
ПК 1.4. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности	<ul style="list-style-type: none"> - обоснование выбранных организационных решений на объектах информатизации; - обоснование мер по внедрению организационных решений на предприятии; 	
ПК 1.5. Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации	<ul style="list-style-type: none"> - обоснование использования носителей конфиденциальной информации; - определение методики обработки и хранения защищаемой информации; - организация выполнения передачи конфиденциальной информации на различных носителях. - полнота и эффективность соблюдения правил использования носителей секретной информации 	
ПК 1.6. Обеспечивать технику безопасности при	<ul style="list-style-type: none"> - определение правил техники безопасности при комплексной защите информации; 	

проведении организационно-технических мероприятий	- определение методики защиты информации при проведении организационно-технических мероприятий.
ПК 1.7. Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите	- обоснование выбранных методов проверок организаций, информация которых подлежит защите; - проведение проверки объектов информатизации; - проведение проверки организаций, работающих с конфиденциальной информацией.
ПК 1.8. Проводить контроль за соблюдением персоналом требований режима защиты информации	- определение методов и способов контроля персонала, работающего с конфиденциальной информацией; - определение последовательности действий при проведении проверок соблюдения персоналом требований режима защиты информации; - организация проведения контроля за работой персонала, задействованного в защите информации организации.
ПК 1.9. Участвовать в оценке качества защиты объекта	- выполнение оценки качества комплексной защиты информации организации; - выполнение оценки качества защиты объекта информатизации; - определение и анализ недостатков качества защиты информации на предприятии.

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности	- демонстрация понимания целей и задач профессиональной деятельности; - осознание способов деятельности, выбор средств, адекватных ее целям и задачам	Отчет по учебной практике
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	- выбор и применение методов и способов решения профессиональных задач в организации и технологии защиты информации; - оценка эффективности и качества выполнения работ.	

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	- рациональность решения стандартных профессиональных задач в области защиты информации; - аргументированность самоанализа выполнения профессиональных задач
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	- эффективный поиск необходимой информации; - использование различных источников, включая электронные
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности	- использование программ автоматизации профессиональной деятельности (владеть навыками работы в специальных программах, а также текстовых и табличных редакторах, программах по созданию презентаций).
ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	- взаимодействие с обучающимися, преподавателями, мастерами, руководителями практик от предприятия в ходе обучения
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий	- самоанализ и коррекция результатов собственной работы при выполнении практических заданий в группе, при подготовке к внеклассным мероприятиям
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	- организация самостоятельных занятий при изучении профессионального модуля
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности	- анализ инноваций в области защиты информации
ОК 10. Применять математический аппарат для решения профессиональных задач.	- уметь применять средства математической логики для решения задач
ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности	- уметь оценивать документы, используемые в области защиты информации
ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих	- проявление интереса к структуре федеральных органов исполнительной власти,

информационную безопасность

обеспечивающих
информационную безопасность.

5. ПЕРЕЧЕНЬ РЕКОМЕНДУЕМЫХ УЧЕБНЫХ ИЗДАНИЙ, ИНТЕРНЕТ-РЕСУРСОВ, ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

Основные источники:

1. Безопасность и упр. доступ. в информ. сист.: Уч. пос. /Васильков А.В., Васильков И.А.-М.:Форум, НИЦ ИНФРА-М, 2017-368с. - 978-5-91134-360-6.
2. Информационная безопасность компьютерных систем и сетей: Уч. пос./В.Ф.Шаньгин -М.: ИД ФОРУМ, НИЦ ИНФРА-М,2018-416с (ПО) ISBN:978-5-8199-0754-2.
3. Организация и технология работы с конфиденциальными документами: Учебник /Зверева В.П., Назаров А.В.-М.:КУРС, НИЦ ИНФРА-М,2018-320с. - 978-5-906818-96-6.