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
Ректор АНПОО «МАНО»
_____ В.И. Гам
«25» июня 2022 г.

РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА

УЧЕБНОЙ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ) ПРАКТИКИ
по профессиональному модулю
ПМ.3 «ПРОГРАММНО-АППАРАТНЫЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»
для специальности
10.02.01 Организация и технология защиты информации

Заочная форма обучения

Омск, 2022

Программа учебной (по профилю специальности) 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: Бугаев А.П., преподаватель.

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ) ПРАКТИКИ

ПМ. 3 Программно-аппаратные и технические средства защиты информации

1.1. Место учебной (по профилю специальности) практики в структуре основной профессиональной образовательной программы

Программа 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): программно-аппаратные и технические средства защиты информации.

1.2. Цель практики

Целью практики является освоение вида профессиональной деятельности «Программно-аппаратные и технические средства защиты информации», закрепление и углубление знаний и умений, формирование общих и профессиональных компетенций, приобретение практического опыта в рамках профессионального модуля ПМ. 3 Программно-аппаратные и технические средства защиты информации

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

иметь практический опыт:

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

уметь:

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

знать:

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

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

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:

5.2.3. Применение программно-аппаратных и технических средств защиты информации.

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

ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации

защищаемых объектов.
ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.
ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.

1.3. Количество часов на освоение программы практики

Рабочая программа рассчитана на прохождение студентами практики в объеме 36 часов.

1.4. Требования к базам практики

Место и время проведения 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. 3 Программно-аппаратные и технические средства защиты информации	**Ознакомление с предприятием и рабочими местами.** 1. Задачи и краткое содержание 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. **Технические методы и средства, технологии защиты информации** 1. Виды потенциальных угроз безопасности информации предприятия. 2. Структура средств перехвата и их функции. 3. Способы предотвращения утечки информации по материально-вещественному каналу. 4. Способы и средства наблюдения. 5. Виды информации, защищаемой техническими средствами. 6. Источники и носители конфиденциальной информации. 7. Источники опасных сигналов. 8. Способы записи информации на различные виды носителей. **Программно-аппаратные средства защиты информации** 1. Виды информации предприятия, защищаемой техническими средствами. 2. Источники и носители конфиденциальной информации. 3. Способы и средства перехвата сигналов. 4. Системы управления доступом в Интернет и контроля корпоративной электронной почты. 5. Проблемы безопасности «виртуальных» инфраструктур. 6. Защита персональных данных, типовые решения. 7. Управление рисками.	36
Итоговая аттестация	Дифференцированный зачет	
		Всего: 36

Задания:

1. Виды, источники и носители защищаемой информации.
2. Источники опасных сигналов.
3. Структура, классификация и основные характеристики технических каналов утечки информации.
4. Классификация технических разведок и методы противодействия им.
5. Методы и средства технической защиты информации.
6. Методы скрытия информации.
7. Программно-аппаратные средства защиты информации.
8. Основные правовые акты в области информационной безопасности и защиты информации.
9. Порядок лицензирования деятельности по технической защите конфиденциальной информации.
10. Правовые нормы в области защиты интеллектуальной собственности.
11. Организация конфиденциального документооборота.
12. Технология работы с конфиденциальными документами
13. Структура подсистемы безопасности операционных систем и выполняемые ею функции.
14. Средства защиты в вычислительных сетях.
15. Средства обеспечения защиты информации в системах управления базами данных.
16. Критерии защищенности компьютерных систем.
17. Методики проверки защищенности объектов информатизации на соответствие требованиям нормативных правовых актов.
18. Работа с техническими средствами защиты информации.
19. Работа с защищёнными автоматизированными системами.
20. Технология передачи информации по защищённым каналам связи.
21. Фиксация отказов в работе средств вычислительной техники.
22. Эксплуатация систем и средств защиты информации защищаемых объектов.
23. Методы выявления угроз информационной безопасности. Выявление и анализ возможных угроз информационной безопасности объектов.

3. ФОРМЫ ОТЧЕТНОСТИ ПО ИТОГАМ УЧЕБНОЙ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ ПРАКТИКИ

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

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ) 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 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.	- анализ научной литературы; - правильный выбор решений по обеспечению инженерно-технической и программной защиты информации; - выбор методов эффективного использования средств обнаружения возможных каналов утечки конфиденциальной информации	Отчет по учебной и производственной практике
ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов	- умение выработать предложения по разработке программ защиты информации на объекте; - умение самостоятельно разрабатывать методики защиты информации на предприятии. - умение самостоятельно применять технические средства защиты информации - определение и анализ недостатков выбранной системы защиты, ее совершенствование.	
ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.	- демонстрация навыков проведения работ по инженерно-технической защите информации; - демонстрация навыков аппаратно-программной защиты информации; -демонстрация навыков регламентных работ по отношению к средствам ЗИ; - фиксация отказов системы защиты.	
ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.	- демонстрация навыков поиска возможных угроз информационной безопасности; -умение самостоятельно выявлять существующие угрозы информационной безопасности; -умение анализировать выявленные угрозы информационной безопасности.	

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 и производственной 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, осознано 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 информационную безопасность	- проявление интереса к структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.	

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

Основные источники:

1. Зверева, В. П. Технические средства информатизации: учебник / В. П. Зверева, А. В. Назаров. - М. : НИЦ ИНФРА, 2017. - 256 с. - 978-5-906818-88-1.
2. Гаврилов, М. В. Информатика и информационные технологии : учебник для СПО / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — М. : Издательство Юрайт, 2017. — 383 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-03051-8.
3. Информационная безоп.комп.систем и сетей: Уч.пос./В.Ф.Шаньгин - М.:ИД ФОРУМ,НИЦ ИНФРА-М,2018-416с - 978-5-8199-0754-2.
4. Бубнов А. А. , Пржегорлинский В. Н. , Савинкин О. А. Основы информационной безопасности: учеб. Пособие, 3-е изд. 2017, 256 с. - 978-5-4468-4651-1.

Дополнительные источники:

1. Белкин П.Ю., Михальский О.О. и др. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учебное пособие для вузов. – М.: Радио и связь, 2011.
2. Васильева И.Н., Стельмашонок Е.В. Информационные технологии и защита информации. Учебное пособие. – СПб, СПбГИЭУ, 2011.
3. Гришина Н.В. Организация комплексной системы защиты информации. – М.: Гелиос АРВ, 2012
4. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2012.
5. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие. – Спб.: НИУ ИТМО, 2012.
6. Мельников В.П. Информационная безопасность: Учебное пособие/ В.П.Мельников, С.А.Клейменов, А.М. Петраков; Под ред.С.А.Клейменова.-6-е изд., Стереотип.-М.: Академия, 2011.
7. Мельников В.П. Информационная безопасность и защита информации: Учебное пособие для студентов высших учебных заведений / В.П.Мельников, С.А.Клейменов, А.М.Петраков; Под ред. С.А.Клейменова.-5-е изд., стер .-М.: Академия, 2011.
8. Сидорин Ю.С. Технические средства защиты информации: Учеб.пособие. – Спб.: Изд-во Политех. ун-та, 2013.
9. Дикарев В.И., Заренков В.А., Заренков Д.В., Койнаш Б.В. Защита объектов и информации от несанкционированного доступа/ Под ред. В.А. Заренкова.– СПб.: ОАО «Издательство Стройиздат СПб», 2009.
10. Емельянова Н.З., Партыка Т.Л., Попов И.И. Защита информации в персональном компьютере: учебное пособие. – М.: Форум, 2009.

11. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2010.
12. Меньшаков Ю.К. Виды и средства иностранных технических разведок: Учеб. пособие/ Под ред. М.П. Сычева.– М.: Изд-во МГТУ им. Н.Э. Баумана, 2009.
13. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки: Учеб. пособие.– М.: Российск. гос. гуманит. ун-т, 2010.
14. Рудометов Е.А., Рудометов В.Е. Электронные средства разведки и защиты информации.– М.: ООО «Фирма «Издательство АСТ»; СПб.: ООО «Издательство ПОЛИГОН», 2008.
15. Степанов Е.А. Защита информации и информационная безопасность. Курс лекций. — М.: Изд-во ГУУ, 2009.
16. Торокин А. А. Инженерно-техническая защита информации: Учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности.– М.: Гелиос АРВ, 2011.
17. Хорев А.А. Техническая защита информации: Учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации.– М.: НПЦ «Аналитика», 2010.