Программа
практики (по профилю специальности)

ПП.03 ПРОИЗВОДСТВЕННАЯ ПРАКТИКА

Вид профессиональной деятельности: программно-аппаратные и технические средства защиты информации

2021 г.

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРАКТИКИ «ПП.03 ПРОИЗВОДСТВЕННАЯ ПРАКТИКА»

1.1. Область применения программы

Программа практики является частью основной профессиональной образовательной программы (далее – ОПОП) в соответствии с ФГОС СПО по специальности 10.02.01 Организация и технология защиты информации в части освоения основного вида профессиональной деятельности (далее – ВПД): программно-аппаратные и технические средства защиты информации.

1.2. Место практики в структуре ОПОП

«ПП.03 Производственная практика» входит в профессиональный модуль «Программно-аппаратные и технические средства защиты информации».

1.3. Цели и задачи программы практики – требования к результатам освоения профессионального модуля

С целью овладения указанным ВПД и соответствующими компетенциями обучающийся в ходе прохождения производственной практики 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.

1.4. Количество часов на освоение программы практики

72 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРАКТИКИ

Результатом освоения программы является овладение обучающимися видом профессиональной деятельности: участие в планировании и организации работ по обеспечению защиты объекта, в том числе профессиональными (далее – ПК) и общими (далее – ОК) компетенциями:

Код	Наименование результата обучения
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.
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.

3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРАКТИКИ

3.1. Структура практики

№ п/п	Разделы (этапы) практики	Виды учебной работы на практике, включая самостоятельную работу обучающихся	Формы текущего контроля обучающихся
1	Подготовительный этап	Организационные собрания, включающие: – распределение по местам прохождения практики; – инструктаж по технике безопасности; – получение индивидуального задания от руководителя практики от колледжа. Прибытие на практику: – согласование структурного подразделения предприятия практики; – инструктаж по технике безопасности; – организация рабочего места; – знакомство с коллективом.	Проверка знаний по технике безопасности.
2	Основной этап	– Определение совместно с руководителем практики от предприятия плана прохождения практики; – выполнение производственных заданий; – мероприятия по сбору, обработке и систематизации материала; – другие виды работ в соответствии с поставленными задачами практики.	Внесение соответствующих записей в дневник практики и отчет. Проверка документов руководителем практики от предприятия. Беседы с руководителями практики от предприятия и колледжа.
3	Заключительный этап	Подготовка отчета.	Устная беседа с руководителем практики. Проверка ведения дневника. Защита отчета.

3.2. Содержание практики

№ п/п	Наименования тем производственной практики	Количество часов
		72
1	Инструктаж по технике безопасности. Организация рабочего места. Знакомство с коллективом.	2
2	1. Создание защищённого канала передачи данных. 2. Настройка идентификации пользователей в автоматизированной системе. 3. Тестирование пожарно-охранной сигнализации. 4. Отслеживание журнала аудита. 5. Проверка системы на вирусы и несанкционированный доступ. 6. Анализ и оценка каналов утечки информации. 7. Исключения несанкционированного доступа к информационным ресурсам. 8. Приемы, методы и способы выявления неисправностей в компьютерах, компьютерных системах и сетях. 9. Описание (моделирования) объектов защиты; 10. Выявление демаскирующих признаков объектов защиты. 11. Использование диагностического оборудования для диагностики технического состояния инженерно-технических средств защиты информации. 12. Использование программно-аппаратных комплексов.	34
3	1. Проверка защищенности объектов информатизации. 2. Осуществление работ с техническими средствами защиты информации. 3. Осуществление работ с защищенными автоматизированными системами. 4. Передача информации по защищенным каналам связи. 5. Выявление возможных угроз информационной безопасности. 6. Использование программно-аппаратных комплексов для диагностики технического состояния инженерно-технических средств защиты информации.	34
4	Защита отчета. Дифференцированный зачёт.	2
Всего		**72**

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРАКТИКИ

4.1. Информационное обеспечение обучения

Основные источники:

1. Внуков А.А. Основы информационной безопасности: защита информации [Электронный ресурс]: учебное пособие для среднего профессионального образования / А.А. Внуков. — М., 2019. — 240 с. — Режим доступа: http://biblio-online.ru/bcode/431332

2. Программно-аппаратные средства защиты информации: учебное пособие / Л.Х. Мифтахова, А.Р. Касимова, В.Н. Красильников и др. – СПб., 2018. – 408 с. – Режим доступа: URL: http://biblioclub.ru/index.php?page=book&id=481123

3. Дербин Е.А., Климов С.М. Организационные основы обеспечения информационной безопасности предприятия: учебное пособие. – М., 2013 – 266 с. – Режим доступа: http://elib.fa.ru/fbook/Elektr_uch._posobie_OOIB1.pdf/download/Elektr_uch._posobie_OOIB1.pdf

4. 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, 2019. — 342 с. — Текст: электронный // URL: http://biblio-online.ru/bcode/431080

Дополнительные источники:

1. Журнал «Защита информации. Инсайд»

2. Программно-аппаратные средства защиты компьютерной информации. Практический курс: учебное пособие / Е.И. Духан, Н.И. Синадский, Д. А. Хорьков; Екатеринбург: УрГУ, 2008, 240 с. – URL: http://elar.urfu.ru/bitstream/10995/1403/5/1331981_schoolbook.pdf

3. Методы и средства защиты компьютерной информации: учебное пособие / А.А. Безбогов, А.В. Яковлев, В.Н. Шамкин. – Тамбов, 2006. – 196 с.– URL: https://www.tstu.ru/book/elib/pdf/2006/shamkin2.pdf

4. Зайцев А.П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. Под ред. А.П. Зайцева, А.А. Шелупанова. - 7-е изд., испр. - М., 2012. - 442 с. – URL: http://www.studentlibrary.ru/book/ISBN9785991202336.html

5. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина - СПб, 2012. - 416 с.– URL: http://window.edu.ru/resource/565/78565

Интернет-ресурсы:

1. Информационно-правовой портал «Гарант» http://www.garant.ru/
2. Справочная правовая система «КонсультантПлюс» http://www.consultant.ru/
3. Федеральный портал «Российское образование» - http://www.edu.ru/
4. Интегральный каталог ресурсов Федерального портала «Российское образование» http://soip-catalog.informika.ru/
5. Федеральный фонд учебных курсов - http://www.ido.edu.ru/ffec/econ-index.html
6. Комплексная система защиты от утечек корпоративной информации - http://www.securit.ru

7. Общественно-государственное объединение «Ассоциация документальной электросвязи» - http://www.rans.ru/

8. Федеральная служба по техническому и экспортному контролю - http://fstec.ru/

4.2. Общие требования к организации образовательного процесса

Практика является обязательным разделом ОПОП. Она представляет собой вид учебных занятий, обеспечивающих практико-ориентированную подготовку обучающихся. Производственная практика проводится в организациях различных организационно-правовых форм на основе договоров между организацией, осуществляющей деятельность по образовательной программе соответствующего профиля, и колледжем.

Аттестация по итогам производственной практики проводится в форме дифференцированного зачета на основании предоставленных отчетов и отзывов с мест прохождения практики.

4.3. Кадровое обеспечение образовательного процесса

Педагогические кадры, осуществляющие руководство практикой имеют опыт деятельности в организациях соответствующей профессиональной сферы. Организацию и руководство производственной практикой осуществляют руководители практики от колледжа и от организации.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

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.	– Обоснованность выбора технических и программно-аппаратных средств защиты информации; – грамотное применение технических и программно-аппаратных средств защиты информации; – правильность освоения возможностей работоспособности компонентов систем защиты информации.	Оценка результатов деятельности обучающихся в процессе освоения образовательной программы: – на практических занятиях (при решении ситуационных задач, участии в деловых играх, при подготовке рефератов, докладов, компьютерных презентаций и т.д.); – при выполнении и защите практических и лабораторных работ; – при выполнении работ на различных этапах учебной и производственной практики; – при проведении тестирования, зачетов, экзаменов, квалификационного экзамена по модулю.
ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.	– Умение решать частные технические задачи, возникающие при эксплуатации систем и средств защиты информации; – умение осуществлять мероприятия по выявлению и оценке свойств каналов утечки информации.	
ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.	– Точность и скорость диагностики нарушений эксплуатационных характеристик средств защиты; – качество анализа эксплуатационных свойств средств защиты; – проверка технического состояния средств защиты; – умения проводить техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность средств защиты.	
ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.	– Умение выявлять и анализировать возможные угрозы информационной безопасности объектов.	

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, проявлять к ней устойчивый интерес.	– Демонстрация интереса к будущей профессии.	Оценка результатов деятельности обучающихся в процессе освоения образовательной программы: – на практических занятиях (при решении ситуационных задач, участии в деловых играх, при подготовке рефератов, докладов, – компьютерных презентаций и т.д.); – при выполнении и защите практических и лабораторных работ; – при выполнении работ на различных этапах производственной практики; – при проведении: тестирования, зачетов, экзаменов, квалификационного экзамена по модулю; – проверка выполнения самостоятельной работы; – защита работ на различных этапах производственной практики.
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 области защиты информации; – оценка эффективности и качества выполнения.	
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	– Решение стандартных и нестандартных профессиональных задач в области защиты информации.	
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.	– Работа с профессиональными информационными системами.	
ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	– Взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения.	
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.	– Самоанализ и коррекция результатов собственной работы.	

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. Исполнять воинскую обязанность, в том числе с применением полученных знаний.	– Готовность к исполнению воинской обязанности с применением полученных профессиональных знаний.	
ОК 11. Применять математический аппарат для решения профессиональных задач.	– Уметь применять средства математической логики для решения задач.	
ОК 12. Оценивать значимость документов, применяемых в профессиональной деятельности.	– Уметь оценивать документы, используемые в области защиты информации.	