

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ «САРОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ ТЕХНИКУМ ИМЕНИ ДВАЖДЫ
ГЕРОЯ СОЦИАЛИСТИЧЕСКОГО ТРУДА БОРИСА ГЛЕБОВИЧА МУЗРУКОВА»

**РАБОЧАЯ ПРОГРАММА
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ**

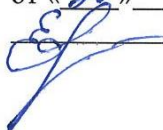
**ПО ПМ.03 ПРИМЕНЕНИЕ ПРОГРАММНО-АППАРАТНЫХ И ТЕХНИЧЕСКИХ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**


для специальности 10.02.01 Организация и технология защиты информации

Программа производственной практики 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: ГБПОУ СПТ им. Б.Г.Музрукова.

Разработчик: И.В. Столяров, преподаватель ГБПОУ СПТ им. Б.Г.Музрукова.

СОГЛАСОВАНО
на МК протокол № 1
от « 30 » 08 2021г.
 /Е.С.Богданович/

УТВЕРЖДАЮ
Зам. директора по УПР
 Е.В.Митянова
« 31 » 08 2021г.

СОДЕРЖАНИЕ

	стр.
1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	4
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	5
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	7
4 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	9
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ	12

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

ПМ.03 Применение программно-аппаратных и технических средств защиты информации

1.1. Область применения рабочей программы

Рабочая программа производственной практики – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности среднего профессионального образования (далее СПО) **10.02.01 Организация и технология защиты информации** в части освоения основного вида профессиональной деятельности (ВПД): **применение программно-аппаратных и технических средств защиты информации** и соответствующих профессиональных компетенций (ПК):

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

Рабочая программа производственной практики может быть использована в дополнительном профессиональном образовании (программы повышения квалификации и переподготовки) и профессиональной подготовке работников в области обеспечения защиты информации.

1.2. Цели и задачи производственной практики – требования к результатам освоения практики

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями студент в ходе освоения 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.

1.3. Условия организации производственной практики

Место проведения: отделения базовых предприятий.

1.4. Рекомендуемое количество часов на освоение программы производственной практики:

Всего: 108 часа, в том числе:

на учебную практику – 108 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Результатом освоения производственной практики является овладение студентами видом профессиональной деятельности (ВПД) **применение программно-аппаратных и технических средств защиты информации**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
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 объектах.
ПК 3.3.	Проводить регламентные работы и фиксировать отказы средств защиты.
ПК 3.4.	Выявлять и анализировать возможные угрозы информационной безопасности объектов.
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес
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

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

3.1. Тематический план производственной практики

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Всего часов	Практика
			Производственная, часов
1	2	3	4
МДК.03.01 Технические методы и средства, технологии защиты информации		284	
ПК 3.1-3.2	Раздел 1. Концепция инженерно-технической защиты информации	30	
ПК 3.1-3.3	Раздел 2. Теоретические основы инженерно-технической защиты информации	24	
ПК 3.1-3.2	Раздел 3. Технические средства добывания и инженерно-технической защиты информации	80	
ПК 3.1-3.2 ПК 3.4	Раздел 4. Организационные основы инженерно-технической защиты информации	18	
ПК 3.3 ПК 3.4	Раздел 5. Технические каналы утечки информации	55	
ПК 3.1- ПК 3.4	Раздел 6. Способы и средства защиты информации от утечки по техническим каналам	30	
ПК 3.1- ПК 3.4	Раздел 7. Методы и средства контроля эффективности технической защиты информации	47	
МДК.03.02 Программно-аппаратные средства защиты информации		360	
ПК 3.3 ПК 3.4	Раздел 1. Подсистемы защиты современных операционных систем	152	
ПК 3.1-3.2 ПК 3.4	Раздел 2. Защита информации в вычислительных сетях	96	
ПК 3.1- ПК 3.4	Раздел 3. Защита информации в системах управления базами данных	62	
ПК 3.1- ПК 3.4	Раздел 4. Антивирусная защита компьютерных систем	50	
	Производственная практика	108	108
	Всего:	752	108

3.2 Содержание обучения производственной практики

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Виды работ (перечень дидактических единиц)	Объем часов	Уровень освоения
1	2	3	4
<p>МДК.03.01 Технические методы и средства, технологии защиты информации</p> <p>МДК.03.02 Программно-аппаратные средства защиты информации</p>	<p>1-3. Проверка защищенности объектов информатизации.</p> <p>4-7.Осуществление работ с техническими средствами защиты информации.</p> <p>8-11.Осуществление работ с защищенными автоматизированными системами.</p> <p>12-13.Передача информации по защищенным каналам связи.</p> <p>14-15.Выявление возможных угроз информационной безопасности.</p> <p>16-17.Использование программно-аппаратных комплексов для диагностики технического состояния инженерно-технических средств защиты информации.</p>	102	2
	Дифференцированный зачет	6	
	Всего	108	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению

Производственная практика проводится как итоговая практика по завершению модуля. Базами производственной практики являются предприятия оборонного комплекса. Основными условиями прохождения производственной практики в данных предприятиях являются наличие квалифицированного персонала, оснащённость современным технологическим оборудованием.

Основные источники:

1. Нестеров С.П. Информационная безопасность: Учебник и практикум для СПО. – М.: Юрвайт, 2019. Электронный ресурс: ЭБС Юрайт <https://bibli-online.ru/viewer/informacionnaya-bezopasnost-442312#page/1>
2. Мельников В.П., Клеймёнов С.А., Петраков А.М. Информационная безопасность: Учеб. пос. Для СПО.- 8-е изд., испр. – М.: Академия, 2013.
3. Платонов В.В. Программно-аппаратные средства защиты информации: Учеб. пос. Для СПО.- 2-е изд., стер. – М.: Академия, 2014.
4. Казарин О. В., Забабурин А. С. Программно-аппаратные средства защиты информации. Защита программного обеспечения: Учебник и практикум для вузов. – М.: Юрвайт, 2019. Электронный ресурс: ЭБС Юрайт <https://bibli-online.ru/viewer/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-437163#page/1>

Дополнительные источники:

1. Торокин А. А. Комплексный технический контроль эффективности мер безопасности систем управления: Учебник. Пособие М.: Гелиос АРВ, 2005.
2. Проскурин В.Г. Защита программ и данных. М.: Издательский центр «Академия», 2011г.
3. Хорев П.Б. методы и средства защиты информации в компьютерных системах. М.: Издательский центр «Академия», 2012г.
4. Девянин П.Н. Программно-аппаратные средства защиты от несанкционированного доступа к компьютерным криптографическим системам обработки информации. М.: РИО МИЭМ, 2013г.
5. Расторуев С.П. программные методы защиты информации в компьютерных сетях. Проблемы информационной безопасности. СПб.: Питер, 2011г.
6. Серегин В.В., Сидоров В.А. Атака через интернет. СПб.: НПО «МИР», 2013г.
7. Спесивцев А.В. защита информации в персональных ЭВМ. М.: Радио и связь, 2012г.

Интернет-ресурсы:

1. Журнал сетевых решений LAN [Электронный ресурс].
URL:<http://www.osp.ru/lan/#/home>
2. Журнал о компьютерных сетях и телекоммуникационных технологиях «Сети и системы связи» [Электронный ресурс].
URL: <http://www.ccc.ru/>
3. <http://www.pandia.ru/>
4. Интернет-Университет Информационных технологий <http://www.intuit.ru/>
5. Закон «Об информации, информационных технологиях и о защите информации» ФЗ N 149-ФЗ от 27 июля 2006 года [Электронный ресурс]/<http://www.rg.ru/Режимдоступа:http://www.rg.ru/2006/07/29/informacia-dok.html>.

4.3. Общие требования к организации производственной практики

Организация практики направлена на выполнение требований к уровню подготовки выпускников в соответствии с получаемой специальностью и присваиваемой квалификацией.

Производственная практика входит в состав ПМ.03 Применение программно-аппаратных и технических средств защиты информации. Базой для освоения данного

профессионального модуля являются такие дисциплины как: Базы данных, Основы информационной безопасности Технические средства информатизации.

Для успешного освоения **ПМ.03 Применение программно-аппаратных и технических средств защиты информации** каждый студент обеспечивается учебно-методическими материалами (тематическими планами практики, учебно-методической литературой, индивидуальными заданиями).

Производственная практика обеспечивает приобретение и закрепление необходимых профессиональных навыков и умений, формирование профессиональных компетенций, готовность к самостоятельной и индивидуальной работе, принятию ответственных решений в рамках профессиональной компетенции.

Производственная практика проводится под руководством преподавателей и специалистов предприятия – базы практики. Руководитель от образовательной организации назначается приказом директора из числа преподавателей специальных дисциплин. В обязанности преподавателя – руководителя практики входит: контроль выполнения программы практики, оказание методической и практической помощи студентам при отработке практических профессиональных умений и приобретения практического опыта, проверка заполнения дневника по производственной практике.

Руководители практики студентов от предприятия - базы практик назначаются приказом руководителя предприятия до начала практики, из числа специалистов имеющих образование, соответствующее профилю преподаваемого профессионального модуля.

Обязательным условием допуска к производственной практике в рамках данного профессионального модуля является освоение теоретического материала.

Во время прохождения производственной практики студент обязан вести дневник – отчет, в котором должен делать записи о проделанной им работе. По материалам практики студент оформляет отчет по форме, разработанной образовательной организацией. В отчет могут быть включены расчеты, эскизы, схемы, графики и чертежи, технологические карты, поясняющие и иллюстрирующие особенности выполненных работ.

Итогом практики является оценка, которая выставляется руководителем практики от образовательной организации на основании оформленного отчета, качества выполнения индивидуального задания, отзыва о работе студента, выданного руководителем практики от предприятия.

В конце изучения профессионального модуля проводится квалификационный экзамен, на который студент представляет дневник практики, отчет и характеристику с места работы.

4.4. Кадровое обеспечение производственной практики

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по профессиональному модулю, включая руководство производственной практикой:

реализация программы подготовки специалистов среднего звена по специальности среднего профессионального образования **10.02.01 Организация и технология защиты информации** обеспечивается педагогическими кадрами, имеющими высшее профессиональное образование, соответствующее профилю преподаваемого профессионального модуля. Преподаватели специальных дисциплин – руководители практики от образовательной организации должны проходить стажировку на базовых предприятиях или в ресурсных центрах образовательных организаций не реже 1 раза в 3 года.

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

5.1 Контроль и оценка результатов освоения профессиональных компетенций

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.	<ul style="list-style-type: none"> - 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. 	<p>Наблюдение за деятельностью студента в процессе учебной практики.</p> <p>Устный опрос.</p> <p>Практическая работа, оценка выполнения практических работ</p> <p>Наблюдение за правильной организацией рабочего места.</p>
ПК.3.2 Участвовать в эксплуатации систем и средств защиты информации защищаемых объектах.	<ul style="list-style-type: none"> - умение решать частные технические задачи, возникающие при эксплуатации систем и средств защиты информации; - умение осуществлять мероприятия по выявлению и оценке свойств каналов утечки информации. 	<p>Собеседование по результатам практики.</p>
ПК.3.3 Проводить регламентные работы и фиксировать отказы средств защиты.	<ul style="list-style-type: none"> - 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. 	<p>Дифференцированный зачет по практике.</p>
ПК.3.4 Выявлять и анализировать возможные угрозы информационной безопасности объектов.	<ul style="list-style-type: none"> - умение выявлять и анализировать возможные угрозы информационной безопасности объектов. 	