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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

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

для специальности 10.02.01 Организация и технология защиты информации

2021 г.

Программа учебной 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

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ
ПМ.03 Применение программно-аппаратных и технических средств защиты информации

1.1.Область применения рабочей программы

Рабочая программа учебной 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 учебной 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 учебной практики – требования к результатам освоения практики

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

Место проведения: лаборатория технических средств обучения; лаборатория электронного документооборота; лаборатория технических и программно-аппаратных средств защиты информации.

1.4. Рекомендуемое количество часов на освоение программы учебной практики:

Всего: 144 часов, в том числе:
на учебную практику – 144 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Результатом освоения учебной 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 УЧЕБНОЙ ПРАКТИКИ

3.1. Тематический план учебной практики

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Всего часов	Практика
			Учебная, 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	
	Учебная практика	**144**	**144**
	Всего:	**788**	**144**

3.2 Содержание обучения учебной практики

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Виды работ (перечень дидактических единиц)	Объем часов	Уровень освоения
1	**2**	**3**	**4**
МДК.03.01 Технические методы и средства, технологии защиты информации **МДК.03.02 Программно-аппаратные средства защиты информации**	1-2.Создание защищённого канала передачи данных. 3-4.Настройка идентификации пользователей в автоматизированной системе. 5-6.Тестирование пожарно- охранной сигнализации. 7-8.Отслеживание журнала аудита. 9-10.Проверка системы на вирусы и несанкционированный доступ. 11-12. Анализ и оценка каналов утечки информации. 13-14. Исключения несанкционированного доступа к информационным ресурсам. 15-16. Приемы, методы и способы выявления неисправностей в компьютерах, компьютерных системах и сетях. 17. Описание (моделирования) объектов защиты; 18-19.Выявление демаскирующих признаков объектов защиты. 20-21.Использование диагностического оборудования для диагностики технического состояния инженерно-технических средств защиты информации 22-23.Использование программно-аппаратных комплексов.	**138**	**2**
	Дифференцированный зачет	**6**	
	Всего	**144**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие:

учебного кабинета

- Информационной безопасности;

лабораторий

- Компьютерной техники**;**
- Электронного документооборота;
- Технических и программно-аппаратных средств защиты информации;

Оборудование учебного кабинета и рабочих мест:

- кабинет Информационной безопасности:
  - посадочные места по количеству обучающихся;
  - рабочее место преподавателя;
  - комплект нормативной документации;
  - плакаты;
  - компьютеры с программным обеспечением;
  - мультимедийные средства обучения.

Оборудование лаборатории и рабочих мест:

- лаборатории: Компьютерной техники**:**
  - посадочные места, рассчитанные на подгруппу, но не менее 8;
  - мультимедийные средства обучения.
  - рабочее место преподавателя;
  - компьютеры с лицензионным программным обеспечением.
- лаборатории: Электронного документооборота:
  - посадочные места, рассчитанные на подгруппу, но не менее 8;
  - мультимедийные средства обучения;
  - рабочее место преподавателя;
  - компьютеры с лицензионным программным обеспечением.
- лаборатории: **Технических и программно-аппаратных средств защиты информации:**
  - посадочные места, рассчитанные на подгруппу, но не менее 8;
  - мультимедийные средства обучения;
  - рабочее место преподавателя;
  - компьютеры с лицензионным программным обеспечением;
  - специализированное программное обеспечение;
  - системы доступа;
  - программно-аппаратные средства защиты информации.

4.2. Информационное обеспечение обучения. Перечень рекомендуемых учебных изданий

Основные источники:

1. Нестеров С.П. Информационная безопасность: Учебник и практикум для СПО. – М.: Юрвайт, 2019. Электронный ресурс: ЭБС Юрайт https://biblio-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://biblio-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 учебной практики

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

Учебная 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.
Обязательным условием допуска к учебной практике в рамках профессионального модуля является освоение студентами всего курса профессионального модуля ПМ.03., сдача практических работ, зачетной работы. В рамках данного модуля проводятся консультации для детального рассмотрения основополагающих аспектов будущей профессии.

4.4. Кадровое обеспечение учебной практики

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по профессиональному модулю, включая руководство учебной 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.	- 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.	Наблюдение за деятельностью студента в процессе учебной практики. Устный опрос. Практическая работа, оценка выполнения практических работ Наблюдение за правильной организацей рабочего

ПК.3.2 Участвовать в эксплуатации систем и средств защиты информации защищаемых объектах.	-умение решать частные технические задачи, возникающие при эксплуатации систем и средств защиты информации; - умение осуществлять мероприятия по выявлению и оценке свойств каналов утечки информации.	места. Собеседование по результатам практики.
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.	Дифференцированный зачет по практике.
ПК.3.4 Выявлять и анализировать возможные угрозы информационной безопасности объектов.	- умение выявлять и анализировать возможные угрозы информационной безопасности объектов.	