

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

РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ПРАКТИКИ
ПО ПМ.01 УЧАСТИЕ В ПЛАНИРОВАНИИ И ОРГАНИЗАЦИИ РАБОТ ПО
ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ОБЪЕКТА


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

	стр.
1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ	4
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ	5
3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ	7
4 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ПРАКТИКИ	9
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ	11

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта

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): **участие в планировании и организации работ по обеспечению защиты объекта и соответствующих профессиональных компетенций (ПК):**

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.

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:

- 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

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: 108 часов, в том числе:
на учебную практику – 108 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Результатом освоения учебной практики является овладение студентами видом профессиональной деятельности (ВПД) **участие в планировании и организации работ по обеспечению защиты объекта**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
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.
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
ПК 1.1 –ПК 1.9.	Раздел 1 Организация системы безопасности предприятия	168	-
	Раздел 2 Работа подразделений защиты информации.	168	
	Раздел 3. Работа персонала с конфиденциальной информацией.	168	
	Учебная практика	108	108
	Всего:	720	108

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
<p>Раздел 1 Организация системы безопасности предприятия</p> <p>Раздел 2 Работа подразделений защиты информации.</p> <p>Раздел 3. Работа персонала с конфиденциальной информацией.</p>	<p>1.Выполнение анализа и обработки распорядительных документов;</p> <p>2. Проведение исследований документов, регламентирующих работу по защите информации;</p> <p>3. Ведение делопроизводства с учетом конфиденциальности информации;</p> <p>4. Проектирование электронной передачи данных, конструктивно-технологических модулей с применением пакетов прикладных программ;</p> <p>5. Разработка комплекта документации;</p> <p>6. Определение показателей надежности и оценка качества хранения конфиденциальных документов на различных носителях;</p> <p>7. Разработка проектной документации с использованием современных пакетов прикладных программ в сфере профессиональной деятельности;</p> <p>8. Инвентаризация объектов, подлежащих защите;</p> <p>9. Изучение требований отчетной документации, используемой при сборе, обработке и передаче конфиденциальной информации;</p> <p>10. Определение всех необходимых правовых документов связанных с защитой информации;</p> <p>11. Выявление методов защиты объектов;</p> <p>12. Сбор материала, необходимого для выработки решений по обеспечению защиты информации;</p> <p>13. Анализ материала для выработки оптимальных решений по обеспечению защиты информации;</p> <p>14. Выявление возможных каналов утечки конфиденциальной информации;</p> <p>15. Выявление зон доступа по типу и степени конфиденциальности работ;</p> <p>16. Использование критериев подбора и расстановки сотрудников подразделений защиты информации;</p> <p>17.Изучение требований к процессу проведения инструктажа персонала по организации работы с конфиденциальной информацией.</p>	102	2
	Дифференцированный зачет	6	
	Всего	108	

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: Ученик и практикум для СПО. – М.: Юрвайт, 2019. Электронный ресурс: ЭБС Юрвайт <https://biblio-2.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. Куняев Н.Н. и др. Конфиденциальное делопроизводство и защищённый электронный документооборот: Учебник для ВУЗов. – М.: ЛОГОС, 2014.
 4. Полякова Т.А. Организационное и правовое обеспечение информационной безопасности: Учебник и практикум для СПО / Отв. ред., Стрельцов А.А. – Юрайт, 2016.
 5. Внуков А. А. Основы информационной безопасности. Защита информации: Учеб. пос. для СПО. – 2-е изд., испр. и доп. - М.: Юрайт, 2019. - Электронный ресурс: ЭБС Юрайт. <https://biblio-online.ru/viewer/osnovy-informacionnoy-bezopasnosti-zaschita-informacii-431332#page/1>

Дополнительные источники:

1. Киселев, С.В. Основы сетевых технологий: учеб. пособие для нач. проф. образования / С.В. Киселев, И.Л. Киселев. – М.: Академия, 2008. – (Непрерывное профессиональное образование).
2. Мельников, В.В. Информационная безопасность: учеб пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков, под. Ред. С.А. Клейменова. – М.: Академия, 2012.
3. Михайлов А.В. Компьютерные вирусы и борьба с ними / А.В. Михайлов . - М.: Диалог-МИФИ, 2011
4. Кузин, А. В. Компьютерные сети: учеб. пособие / А.В. Кузин, В.М. Демин. – М.: Форум, 2008.
5. Петренко С.А. Политики информационной безопасности / С.А. Петренко, В. А. Курбатов. - М.: Академия АйТи, 2011

Интернет ресурсы:

1. Бесплатный для студентов, аспирантов, школьников и преподавателей доступ к полным лицензионным версиям инструментов Microsoft для разработки и дизайна - <http://www.dreamspark.ru/>
 2. Интернет-Университет Информационных технологий <http://www.intuit.ru/>
- Закон «Об информации, информационных технологиях и о защите информации» ФЗ N 149-ФЗ от 27 июля 2006 года [Электронный ресурс]/ <http://www.rg.ru/> Режим доступа:<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.01 Участие в планировании и организации работ по обеспечению защиты объекта.**

Базой для освоения данного профессионального модуля являются такие дисциплины как: Базы данных, Основы информационной безопасности Технические средства информатизации. Для успешного освоения **ПМ.01 Участие в планировании и организации работ по обеспечению защиты объекта** 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.01., 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
ПК1.1 Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.	- грамотная организация сбора и обработки материалов; - эффективное использование средств обнаружения возможных каналов утечки конфиденциальной информации.	Наблюдение за деятельностью студента в процессе учебной практики. Устный опрос. Практическая работа, оценка выполнения практических работ
ПК1.2 Участвовать в разработке программ и методик организации защиты информации на объекте.	- правильность использования методик организации защиты информации на объекте; - умение разрабатывать программы по защите информации на объекте.	Наблюдение за правильной организацией рабочего места. Собеседование по результатам практики.
ПК1.3 Осуществлять планирование и организацию выполнения мероприятий по	- грамотное планирование мероприятий по защите информации;	Дифференцированный

зачет по практике.

защите информации.	- правильная организация выполнения мероприятий по защите информации.
ПК 1.4 Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.	-соблюдение корпоративной этики; - умение принимать организационные решения на объектах профессиональной деятельности.
ПК1.5 Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации.	-грамотное ведение учета, обработки, хранения, передачи, использования различных носителей конфиденциальной информации.
ПК1.6 Обеспечивать технику безопасности при проведении организационно-технических мероприятий.	- соблюдение техники безопасности при проведении организационно-технических мероприятий.
ПК1.7 Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.	- грамотная организация и проведение проверок объектов информатизации, подлежащих защите.
ПК1.8 Проводить контроль соблюдения персоналом требований режима защиты информации.	- правильность проведения контроля соблюдения персоналом требований режима защиты информации.
ПК1.9 Участвовать в оценке качества защиты объекта.	- грамотная оценка качества защиты объекта.