

ГОСУДАСТВЕННОЕ ПРОФЕССИОНАЛЬНОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ  
«НИЖЕГОРОДСКИЙ ПРОМЫШЛЕННО- ТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ  
специальность 10.02.01 Организация и технология защиты  
информации

Нижний Новгород  
2020 г

Рабочая программа учебной практики разработана на основе Федерального государственного образовательного стандарта специальности среднего профессионального образования 10.02.01 Организация и технология защиты информации.

**Организация-разработчик:**

ГБПОУ «Нижегородский промышленно- технологический техникум»

## **СОДЕРЖАНИЕ**

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ
3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

ПРИЛОЖЕНИЯ

# 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

## 1.1. Область применения программы

Рабочая программа учебной практики является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности 10.02.01 Организация и технология защиты информации.

**1.2. Цели и задачи учебной практики:** формирование у студентов первоначальных практических профессиональных умений в рамках модулей ОПОП СПО по основным видам профессиональной деятельности для освоения рабочей профессии, обучение трудовым приемам, операциям и способам выполнения трудовых процессов, характерных для соответствующей специальности и необходимых для последующего освоения ими общих и профессиональных компетенций по избранной профессии.

## Требования к результатам освоения учебной практики

**С целью овладения указанным видам профессиональной деятельности и соответствующими профессиональными компетенциями обучающиеся в ходе освоения учебной практики УП 01. По профессиональному модулю ПМ01 Участие в планировании и организации работ по обеспечению защиты объекта 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.

**С целью овладения указанным видам профессиональной деятельности и соответствующими профессиональными компетенциями обучающиеся в ходе освоения учебной практики УП 02. По профессиональному модулю ПМ02 Организация и технология работы с конфиденциальными документами:**

**иметь практический опыт:**

- ведения учета и оформления бумажных и машинных носителей конфиденциальной информации;
- работы с информационными системами электронного документооборота;

**уметь:**

- использовать в профессиональной деятельности нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации;
- документировать ход и результаты служебного расследования;
- определять состав документируемой конфиденциальной информации;
- подготавливать, издавать и учитывать конфиденциальные документы;
- составлять номенклатуру конфиденциальных дел;
- формировать и оформлять конфиденциальные дела;
- организовывать и вести конфиденциальное делопроизводство, в том числе с использованием вычислительной техники;
- использовать системы электронного документооборота;

**знать:**

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
- правовые основы защиты конфиденциальной информации по видам тайны;
- порядок лицензирования деятельности по технической защите конфиденциальной информации;
- правовые основы деятельности подразделений защиты информации;
- правовую основу допуска и доступа персонала к защищаемым сведениям;
- правовое регулирование взаимоотношений администрации и персонала в области защиты информации;
- систему правовой ответственности за утечку информации и утрату носителей информации;
- правовые нормы в области защиты интеллектуальной собственности;
- порядок отнесения информации к разряду конфиденциальной информации;
- порядок разработки, учета, хранения, размножения и уничтожения конфиденциальных документов;
- организацию конфиденциального документооборота;
- технологию работы с конфиденциальными документами;

- организацию электронного документооборота

**С целью овладения указанным видам профессиональной деятельности и соответствующими профессиональными компетенциями обучающиеся в ходе освоения учебной практики УП 03. По профессиональному модулю ПМ03 Программно-аппаратные и технические средства защиты информации:**

**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.

**С целью овладения указанным видам профессиональной деятельности и соответствующими профессиональными компетенциями обучающиеся в ходе освоения учебной практики УП 04. По профессиональному модулю ПМ 04. Выполнение работ по профессии оператор электронно- вычислительных и вычислительных машин:**

**иметь практический опыт:**

- подключения кабельной системы персонального компьютера, периферийного и мультимедийного оборудования;
- настройки параметров функционирования персонального компьютера, периферийного и мультимедийного оборудования;
- ввода цифровой и аналоговой информации в персональный компьютер с различных носителей, периферийного и мультимедийного оборудования;
- сканирования, обработки и распознавания документов;
- конвертирования медиафайлов в различные форматы, экспорта и импорта файлов в различные программы-редакторы

- обработки аудио-, визуального и мультимедийного контента с помощью специализированных программ-редакторов;
- создания и воспроизведения видеороликов, презентаций, слайд-шоу, медиафайлов и другой итоговой продукции из исходных аудио-визуальных и мультимедийных компонентов;
- осуществления навигации по ресурсам, поиска, ввода и передачи данных с помощью технологий и сервисов сети Интернет;
- управления медиатекой цифровой информации;
- передачи и размещения цифровой информации;
- тиражирования мультимедиа контента на съемных носителях информации;
- осуществления навигации по ресурсам, поиска, ввода и передачи данных с помощью технологий и сервисов сети Интернет;
- публикации мультимедиа контента в сети Интернет;
- обеспечения информационной безопасности;

**уметь:**

- подключать и настраивать параметры функционирования персонального компьютера, периферийного и мультимедийного оборудования;
  - настраивать основные компоненты графического интерфейса операционной системы и специализированных программ-редакторов;
  - управлять файлами данных на локальных, съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в сети Интернет;
  - производить распечатку, копирование и тиражирование документов на принтере и других периферийных устройствах вывода;
  - распознавать сканированные текстовые документы с помощью программ распознавания текста;
  - вводить цифровую и аналоговую информацию в персональный компьютер с различных носителей, периферийного и мультимедийного оборудования
  - создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики;
  - конвертировать файлы с цифровой информацией в различные форматы;
  - производить сканирование прозрачных и непрозрачных оригиналов;
  - производить съемку и передачу цифровых изображений с фото- и видеокамеры на персональный компьютер;
  - обрабатывать аудио, визуальный контент и медиафайлы средствами звуковых, графических и видео-редакторов;
- 
- создавать видеоролики, презентации, слайд-шоу, медиафайлы и другую итоговую продукцию из исходных аудио, визуальных и мультимедийных компонентов;
  - воспроизводить аудио, визуальный контент и медиафайлы средствами персонального компьютера и мультимедийного оборудования;
  - производить распечатку, копирование и тиражирование документов на принтере и других периферийных устройствах вывода;
  - использовать мультимедиа-проектор для демонстрации содержимого экранных форм с персонального компьютера;
  - вести отчетную и техническую документацию;
  - подключать периферийные устройства и мультимедийное оборудование к персональному компьютеру и настраивать режимы их работы;
  - создавать и структурировать хранение цифровой информации в медиатеке персональных компьютеров и серверов;
  - передавать и размещать цифровую информацию на дисках персонального компьютера, а также дисковых хранилищах локальной и глобальной компьютерной сети;

- тиражировать мультимедиа контент на различных съемных носителях информации;
  - осуществлять навигацию по веб-ресурсам Интернета с помощью веб-браузера;
  - создавать и обмениваться письмами электронной почты;
  - публиковать мультимедиа контент на различных сервисах в сети Интернет;
  - осуществлять резервное копирование и восстановление данных;
  - осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ;
  - осуществлять мероприятия по защите персональных данных;
  - вести отчетную и техническую документацию;
- знать:**
- устройство персональных компьютеров, основные блоки, функции и технические характеристики;
  - архитектуру, состав, функции и классификацию операционных систем персонального компьютера;
  - виды и назначение периферийных устройств, их устройство и принцип действия, интерфейсы подключения и правила эксплуатации;
  - принципы установки и настройки основных компонентов операционной системы и драйверов периферийного оборудования;
  - принципы цифрового представления звуковой, графической, видео и мультимедийной информации в персональном компьютере;
  - виды и параметры форматов аудио-, графических, видео- и мультимедийных файлов и методы их конвертирования;
  - назначение, возможности, правила эксплуатации мультимедийного оборудования;
  - основные типы интерфейсов для подключения мультимедийного оборудования;
  - основные приемы обработки цифровой информации;
  - назначение, разновидности и функциональные возможности программ обработки звука;
  - назначение, разновидности и функциональные возможности программ обработки графических изображений;
  - назначение, разновидности и функциональные возможности программ обработки видео- и мультимедиа контента;
  - принципы лицензирования и модели распространения мультимедийного контента;
  - нормативные документы по установке, эксплуатации и охране труда при работе с персональным компьютером, периферийным оборудованием и компьютерной оргтехникой;
  - структуру, виды информационных ресурсов и основные виды услуг в сети Интернет;
  - назначение, разновидности и функциональные возможности программ для создания веб-страниц; нормативные документы по охране труда при работе с персональным компьютером, периферийным, мультимедийным оборудованием и компьютерной оргтехникой
  - назначение, разновидности и функциональные возможности программ для публикации мультимедиа контента;
  - принципы лицензирования и модели распространения мультимедийного контента;
  - нормативные документы по установке, эксплуатации и охране труда при работе с персональным компьютером, периферийным оборудованием и компьютерной оргтехникой;
  - структуру, виды информационных ресурсов и основные виды услуг в сети Интернет;
  - основные виды угроз информационной безопасности и средства защиты информации; принципы антивирусной защиты персонального компьютера;
  - состав мероприятий по защите персональных данных.

### 1.3. Количество часов на освоение рабочей программы учебной практики:



Всего - 540 часа, в том числе:

В рамках освоения ПМ 01. – 72 часа

В рамках освоения ПМ 02 - 108 часов

В рамках освоения ПМ 03 – 288 часа

В рамках освоения ПМ 04- 72 часа

## 2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

## 2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Результатом освоения рабочей программы учебной практики является сформированность у обучающихся первоначальных практических профессиональных **умений** в рамках модулей ОПОП СПО по основным видам профессиональной деятельности (ВПД): проведение работ по документационному и организационно-технологическому обеспечению защиты информации в организациях различных структур и отраслевой направленности.

(ПК) и общих компетенций (ОК):

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 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.
ПК 2.1	Участвовать в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации
ПК 2.2	Участвовать в организации и обеспечивать технологию ведения делопроизводства с учетом конфиденциальности информации
ПК 2.3	Организовывать документооборот, в том числе электронный, с учетом конфиденциальности информации
ПК 2.4	Организовывать архивное хранение конфиденциальных документов.
ПК 2.5	Оформлять документацию по оперативному управлению средствами защиты информации и персоналом.
ПК 2.6	Вести учет работ и объектов, подлежащих защите.
ПК 2.7	Подготавливать отчетную документацию, связанную с эксплуатацией средств контроля и защиты информации.
ПК 2.8	Документировать ход и результаты служебного расследования
ПК 2.9	Использовать нормативные правовые акты, нормативно-методические документы по защите 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.
ПК 4.1	Подготавливать к работе и настраивать аппаратное обеспечение, периферийные устройства, операционную систему персонального компьютера и мультимедийное оборудование.
ПК 4.2.	Выполнять ввод цифровой и аналоговой информации в персональный компьютер с различных носителей.
ПК 4.3.	Конвертировать файлы с цифровой информацией в различные форматы.
ПК 4.4.	Обрабатывать аудио и визуальный контент средствами звуковых, графических и видео-редакторов.
ПК 4.5.	Создавать и воспроизводить видеоролики, презентации, слайд-шоу, медиафайлы и другую итоговую продукцию из исходных аудио, визуальных и мультимедийных компонентов средствами персонального компьютера и мультимедийного оборудования.

### 3. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

#### 3.1. Тематический план учебной практики

Код ПК	Код и наименования профессиональных модулей	Количество часов по ПМ	Наименования тем учебной практики	Количество часов по темам
1	2	3	4	5
ПК 1.1 ПК1.2 ПК 1.3 ПК 1.4 ПК.1.5 ПК.1.6 ПК.1.7 ПК.1.8 ПК.1.9	ПМ.01 Участие в планировании работ по обеспечению защиты объекта	72	Тема 1. Общие положения концепции обеспечения безопасности информации в системе организации.	6
Тема 2. Угрозы безопасности информации организации.			6	
Тема 3. Задачи обеспечения безопасности информации.			6	
Тема 4. Принципы построения системы комплексной защиты информации.			6	
Тема 5. Участие в планировании и организации работ по обеспечению защиты объекта:			24	
Тема 6. Организация и технология работы с конфиденциальными документами			18	
Промежуточная аттестация в форме дифференцированного зачета			6	

<b>Итого в рамках изучения ПМ 01.</b>			<b>72</b>	
<b>ПК 2.1</b>	<b>ПМ02 Организация и технология работы с конфиденциальными документами</b>	<b>108</b>	Тема 1. Информация как объект правового регулирования Законодательство в области информационной безопасности.	6
<b>ПК2.2</b>			Тема 2. Правовой режим защиты государственной тайны. Правовые режимы защиты конфиденциальной информации	6
<b>ПК 2.3</b>			Тема 3. Лицензирование и сертификация в информационной сфере.	6
<b>ПК 2.4</b>			Тема 4. Защита интеллектуальной собственности.	6
<b>ПК2.5</b>			Тема 5. Практические вопросы документа и документооборота в информационных технологиях.	6
<b>ПК 2.6</b>			Тема 6. Международное законодательство в области защиты информации.	6
<b>ПК 2.7</b>			Тема 7. Понятие и особенности конфиденциальной информации. Общая характеристика нормативной правовой базы. Документирование конфиденциальной информации (организация конфиденциального делопроизводства)	6
<b>ПК 2.8</b>			Тема 8. Организация конфиденциального документооборота. Разрешительная система доступа к конфиденциальной информации	6
<b>ПК 2.9</b>			Тема 9. Составление номенклатуры дел, формирование и оформление конфиденциальных дел. Подготовка конфиденциальных документов к архивному хранению или уничтожению.	6

			Тема 10. Режим конфиденциальности документированной информации.	6
			Тема 11. Предмет и содержание курса	
			Тема 12. Понятие системы Документационного Обеспечения Управления (СДОУ)	6
			Тема 13. Понятие формы электронного документа (ЭД)	6
			Тема 14. Проектирование систем ввода потоков входящих документов	6
			Тема 15. Проектирование систем управления документами	6
			Тема 16. Проектирование системы электронного документооборота. Электронная цифровая подпись	6
			Тема 17. Бизнес-процессы в документообороте. Автоматизированные информационные системы как средства обработки и хранения документов	6
			Тема 18 Проектирование системы электронного документооборота в программе MS Outlook. Вопросы экономической эффективности от внедрения СЭДО	6
			Промежуточная аттестация в форме дифференцированного зачета	6
<b>Итого в рамках изучения ПМ 02.</b>				<b>108</b>
<b>ПК 3.1</b> <b>ПК 3.2</b>	<b>ПМ.03 Применение программно-аппаратных и</b>	<b>288</b>	Тема 1. Применение программно-аппаратных и инженерно-технических средств защиты информации:	282

<b>ПК 3.3</b>	<b>технических средств защиты информации</b>		Промежуточная аттестация в форме дифференцированного зачета	6
<b>ПК 3.4</b>				
<b>Итого в рамках изучения ПМ 03.</b>				<b>288</b>
<b>ПК 4.1</b>	<b>ПМ 04. Выполнение работ по профессии оператор электронно-вычислительных и вычислительных машин.</b>	<b>72</b>	Тема 1. Введение. Понятие мультимедиа.	6
<b>ПК4.2</b>			Тема 2. Аппаратные компоненты мультимедиа. Программное обеспечение	6
<b>ПК 4.3</b>			Тема 3. Технология обработки цифровой информации.	6
<b>ПК 4.4</b>			Тема 4. Конвертирование файлов в различные форматы.	6
<b>ПК.4.5</b>			Тема 5. Ввод и обработка звука на компьютере. Ввод и обработка видео на компьютере. Технология обработки графической информации	6
			Тема 6. Технологии создания мультимедийных презентаций. Ввод и обработка цифрового фото	6
			Тема 7. Принцип создания медиатеки. Размещение цифровой информации	6
			Тема 8. Организация структуры хранения данных. Правовые основы копирования и хранения информации	6
			Тема 9. Основные виды угроз информационной безопасности. Средства защиты информации. Принцип антивирусной защиты ПК.	6



		Тема 10. Структура сети Интернет. Основные виды услуг в сети Интернет	6
		Тема 11. Язык гипертекстовой разметки HTML	6
		Промежуточная аттестация в форме дифференцированного зачета	6
<b>Итого в рамках изучения ПМ 04.</b>			<b>72</b>
<b>Итого</b>			<b>540</b>

### 3.2. Содержание учебной практики

Код и наименование профессиональных модулей и тем учебной практики	Содержание учебных занятий	Объем часов	Уровень освоения
1	2	3	
<b>ПМ 01. Участие в планировании работ по обеспечению защиты объекта</b>		<b>72</b>	<b>3</b>
Тема 1. Общие положения концепции обеспечения безопасности информации в системе организации.	Вводный инструктаж. Знакомство с правилами внутреннего распорядка, рабочим местом и руководителем практики.	6	
Тема 2. Угрозы безопасности информации организации.	Анализ степеней угроз защиты информации, выявления различных видов угроз. Выявление и анализ мер по нейтрализации действий сотрудников организации, приводящих к частичному или полному отказу системы.	6	
Тема 3. Задачи обеспечения безопасности информации.	Выявление и анализ объектов защиты информации условного предприятия. Выявление задач по обеспечению защиты информации и путей достижения целей защиты	6	

<p>Тема 4.</p> <p>Принципы построения системы комплексной защиты информации.</p>	<p>Составление технического регламента о порядке оформления допуска лиц к конфиденциальным сведениям. Составление технического регламента работы с системой внешнего видеонаблюдения. Составление технического регламента работы с системой внутреннего видеонаблюдения. Составление технического регламента организации и проведения рабочих совещаний.</p>	<p>6</p>	
<p>Тема 5.</p> <p>Участие в планировании и организации работ по обеспечению защиты объекта:</p>	<p>Участие в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации. Участие в разработке программ и методик организации защиты информации на объекте</p>	<p>6</p>	
	<p>Осуществлять планирование и организацию выполнения мероприятий по защите информации. Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности</p>	<p>6</p>	
	<p>Ведение учета, обработки, хранения, передачи, использование различных носителей конфиденциальной информации. Обеспечение техники безопасности при проведении организационно-технических мероприятий</p>	<p>6</p>	
	<p>Участие в организации и проведении проверок объектов информатизации, подлежащих защите. Контроль соблюдения персоналом требований режима защиты информации. Участие в оценке качества защиты объекта</p>	<p>6</p>	

Тема 3.1. Организация и технология работы с конфиденциальными документами:	Участие в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации. Участие в организации и обеспечение технологии ведения делопроизводства с учетом конфиденциальности информации	6	
	Организация документооборота, в том числе электронного, с учетом конфиденциальности информации. Организация архивного хранения конфиденциальных документов. Оформление документации по оперативному управлению средствами защиты информации. Учет работ и объектов, подлежащих защите. Подготовка отчетной документации, связанной с эксплуатацией средств контроля и защиты информации	6	
	Документирование хода и результатов служебного расследования. Использование нормативных правовых актов, нормативно-методических документов по защите информации	6	
<b>Дифференцированный зачет</b>		6	
<b>Итого ПМ 01.</b>		<b>72</b>	
<b>Раздел ПМ02 Организация и технология работы с конфиденциальными документами</b>			3
Тема 1. Информация как объект правового регулирования Законодательство в области информационной безопасности.	Вводный инструктаж. Знакомство с работой организации, учреждения. Ознакомление с правилами внутреннего распорядка, рабочим местом и руководителем практики.	6	

<p>Тема 2. Правовой режим защиты государственной тайны. Правовые режимы защиты конфиденциальной информации</p>	<p>Сбор и обработка материалов для выработки решений по обеспечению защиты информации.</p> <p>Требования и технологические аспекты учета, виды и формы, состав сведений и процедуры выполнения.</p> <p>Учет конфиденциальных документов в учетных формах открытого делопроизводства.</p> <p>Отнесение информации к разряду конфиденциальной информации по категории доступа.</p>	<p>6</p>	
<p>Тема 3. Лицензирование и сертификация в информационной сфере.</p>	<p>Засекречивание сведений и их носителей. Грифы секретности и реквизиты носителей сведений, составляющих тайну.</p>	<p>6</p>	
<p>Тема 4. Защита интеллектуальной собственности.</p>	<p>Участие в подготовке организационных и распорядительных документов, регламентирующих работу по защите информации.</p> <p>Перечень поступивших документов и ведение журнала передачи конфиденциальных документов</p>	<p>6</p>	
<p>Тема 5. Практические вопросы документа и документооборота в информационных технологиях.</p>	<p>Проведение учета различных носителей конфиденциальной информации, работ и объектов, подлежащих защите.</p> <p>Порядок работы и требования по работе с документами. Обязанности исполнителей. Состав исполнителей.</p>	<p>6</p>	
<p>Тема 6. Международное законодательство в области защиты информации.</p>	<p>Разрешительная система доступа и запреты. Фиксация прохождения документа и проверка комплектности</p>	<p>6</p>	

<p>Тема 7. Понятие и особенности конфиденциальной информации. Общая характеристика нормативной правовой базы. Документирование конфиденциальной информации (организация конфиденциального делопроизводства)</p>	<p>Изучение и модернизация технологии ведения конфиденциального делопроизводства.</p> <p>Хранение конфиденциальных документов в подразделениях конфиденциального делопроизводства и в архивах предприятия.</p> <p>Режим хранения.</p> <p>Расположение помещений.</p> <p>Нормы хранения документов.</p> <p>Санитарные, пожарные требования к физической сохранности документов.</p>	6	
<p>Тема 8. Организация конфиденциального документооборота. Разрешительная система доступа к конфиденциальной информации</p>	<p>Организация документооборота, в том числе электронного (при наличии в организации), с учетом конфиденциальности информации.</p> <p>Экспертиза ценности документов, ее периодичность.</p> <p>Задачи и функции экспертной комиссии.</p>	6	
<p>Тема 9. Составление номенклатуры дел, формирование и оформление конфиденциальных дел.</p>	<p>Определение сроков хранения и уничтожения документов, дел, носителей конфиденциальной информации.</p> <p>Составление описей дел.</p>	6	

Подготовка конфиденциальных документов к архивному хранению или уничтожению.			
Тема 10. Режим конфиденциальности документированной информации.	Оформление документации по оперативному управлению средствами защиты информации и персоналом, имеющим доступ к конфиденциальным сведениям.	6	
Тема 11. Предмет и содержание курса  Тема 12. Понятие системы Документационного Обеспечения Управления (СДОУ)	Источники конфиденциальной информации (каналы утечки информации) на предприятии, угрозы безопасности конфиденциальной информации, источники угроз, цели и способы реализации угроз.	6	
Тема 13. Понятие формы электронного документа (ЭД)	Подготовка отчетной документации, связанной с эксплуатацией средств контроля и защиты информации.  Основные положения Руководящих документов ГТК в области защиты информации	6	
Тема 14. Проектирование систем ввода потоков входящих документов	Систематизация и ознакомление с результатами служебных расследований за прошлые годы. Порядок приобретения, установки и сертификации систем конфиденциального электронного документооборота и делопроизводства.	6	

Тема 15. Проектирование систем управления документами	Проектирование систем управления документами	6	
Тема 16. Проектирование системы электронного документооборота. Электронная цифровая подпись	Регулирование взаимоотношений администрации и персонала в области защиты информации	6	
Тема 17. Бизнес-процессы в документообороте. Автоматизированные информационные системы как средства обработки и хранения документов	Автоматизирование информационных систем как средства обработки и хранения документов	6	
Тема 18 Проектирование системы электронного документооборота в программе MS Outlook. Вопросы экономической эффективности от внедрения СЭДО	Проектирование системы электронного документооборота в программе MS Outlook. Создание, учета, обработки и исполнения документов, ознакомление с результатами служебных расследований.	6	
	<b>Дифференцированный зачет</b>	6	
<b>Итого ПМ 02</b>		<b>108</b>	



<b>ПМ 03. Применение программно-технических средств защиты информации.</b>			
Тема 1.			<b>3</b>
Применение программно-аппаратных и инженерно-технических средств защиты информации:	Применение программно-аппаратных и технических средств защиты информации на защищаемых объектах	12	
	Настройка систем защиты информации	12	
	Участие в эксплуатации систем и средств защиты информации защищаемых объектов	12	
	Выявление и анализ возможных угроз информационной безопасности объектов	12	
	Проведение регламентных работ и фиксация отказов средств защиты	12	
	Проведение регламентных работ по проверке систем защиты информации	12	
	Подбор и применение программно-аппаратных и технических средств защиты информации	12	
	Подготовка проекта выделения зон доступа по типу работ на объекте	12	
	Подготовка проекта выделения зон доступа по конфиденциальности работ объекте	12	
	Подготовка проекта установки СКУД на объекте	12	
	Составление технического регламента работы с СКУД объекта	12	
	Составление Положения об охране персонала объекта	12	
	Составление Положения о режимных помещениях объекта	12	
	Подготовка проекта оборудования режимного помещения объекта	12	
	Проведение исследования о целесообразности внедрения биометрических систем безопасности на объекте	12	
	Проведение технического аудита системы видеонаблюдения объекта	12	
	Проведение технического аудита СКУД объекта	12	

	Проведение технического аудита безопасности компьютерных систем объекта	12	
	Составление Положения о подразделении защиты информации	12	
	Составление Положения о проверке персонала по защите информации	6	
	Составление технического регламента работы с компьютерными системами объекта	12	
	Составление технического регламента защиты информации в процессе рекламной деятельности	12	
	Проведение технического аудита организации охраны объекта	12	
	Проведение исследования о соответствии подбора и расстановки сотрудников подразделений защиты информации	12	
	<b>Дифференцированный зачет</b>	6	
<b>Итого ПМ 03.</b>		<b>288</b>	
<b>ПМ 04. Выполнение работ по одной или нескольким профессиям</b>			
Тема 1. Введение. Понятие мультимедиа.	Ознакомление с оборудованием компьютерного класса, Т.Б при работе с оборудованием.  Работа с формами подачи мультимедийного контента.	6	<b>3</b>
Тема 2. Аппаратные компоненты мультимедиа. Программное обеспечение	Подключение кабельной системы ПК а и периферийного оборудования; работа с мультимедиа-проектором и офисным оборудованием..Настраивание основных компонентов графического интерфейса ОС и специализированных программ-редакторов.	6	
Тема 3. Технология обработки цифровой информации.	Ввод текстовой информации, создание отчетной и технической документации, сканирование и распознавание сканированных документов, обработка мультимедиа-контента;	6	2

Тема 4. Конвертирование файлов в различные форматы.	Конвертирование файлов с цифровой информацией в различные форматы;	6	2
Тема 5. Ввод и обработка звука на компьютере. Ввод и обработка видео на компьютере. Технология обработки графической информации	Ввод, воспроизведение и редактирование аудиоинформации. Ввод, воспроизведение и редактирование видеоинформации. Ввод графической информации с различных носителей, создание и редактирование графических объектов растровой и векторной графики.	6	2
Тема 6. Технологии создания мультимедийных презентаций. Ввод и обработка цифрового фото	Съемка и передача цифровых изображений, создание видеороликов, презентаций, слайд-шоу, медиа-файлов. Ввод цифровых изображений с различных носителей, обработка цифровых изображений при помощи редакторов.	6	2
Тема 7. Принцип создания медиатеки. Размещение цифровой информации	Изучение функционала различных программ для публикации мультимедиа контента.	6	2

	Передача и размещение цифровой информации. Обеспечение информационной безопасности.	<b>6</b>	<b>2</b>
Тема 8. Организация структуры хранения данных. Правовые основы копирования и хранения информации	Разработка политики безопасности, создание резервных копий мультимедиа контента.	<b>6</b>	<b>2</b>
Тема 9. Основные виды угроз информационной безопасности. Средства защиты информации. Принцип антивирусной защиты ПК.	Изучение возможностей альтернативного антивирусного программного обеспечения, проведение антивирусной профилактики вычислительной техники.	<b>6</b>	
Тема 10. Структура сети Интернет. Основные виды услуг в сети Интернет	Изучение строения сайтов, осуществление навигации по ресурсам, поиска, ввода и передачи данных с помощью технологий и сервисов сети Интернет.	<b>6</b>	<b>2</b>
Тема 11. Язык гипертекстовой разметки HTML	Изучение строения сайтов. Работа с языком гипертекстовой разметки HTML с помощью встроенных в ОС редакторов, создание Веб-документов средствами Microsoft Office , работа с конструкторами для создания сайтов, публикация созданных проектов в сети Интернет.	<b>6</b>	

	<b>Дифференцированный зачет</b>	<b>6</b>	
<b>Итого ПМ 04</b>		<b>72</b>	

## **4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ**

### **4.1. Требования к минимальному материально-техническому обеспечению**

Реализация учебной практики предполагает наличие:

Кабинетов: информационной безопасности;

Лабораторий: компьютерной техники; электронного документооборота; технических средств защиты  
Оборудование лабораторий и рабочих мест:

Оборудование:

- автоматизированное рабочее место преподавателя;
- посадочные места обучающихся (по количеству обучающихся);
- маркерная доска;
- компьютеры (рабочие станции);
- принтер;
- сканер;
- средства физической защиты информации;
- объекты видеонаблюдения;
- USB-накопители;
- наушники;
- локальная сеть;
- мультимедийный класс;
- комплект учебно-методической документации;
- комплект нормативно-правовой документации;
- лицензионное программное обеспечение.

Технические средства обучения:

- рабочее место преподавателя, оснащенное компьютером с лицензионным программным обеспечением, мультимедиапроектором и электронной доской.
- обучающие видеофильмы, презентации.

### **4.2. Информационное обеспечение обучения**

#### **Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы**

Основные источники:

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMAR.
2. Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гультяева. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — Текст : электронный // Цифровой

образовательный ресурс IPR SMART.

3. Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Ю. Н. Рагозин ; под редакцией Т. С. Кулаковой. — Санкт-Петербург : Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART.
4. Майстренко, А. В. Мультимедийные средства обработки информации : учебное пособие для СПО / А. В. Майстренко, Н. В. Майстренко. — Саратов : Профобразование, 2020. — 81 с. — ISBN 978-5-4488-0734-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS.
5. Соловьев, Н. А. Цифровая обработка информации в задачах и примерах : учебное пособие для СПО / Н. А. Соловьев, Н. А. Тишина, Л. А. Юркевская. — Саратов : Профобразование, 2020. — 122 с. — ISBN 978-5-4488-0596-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS.
6. Скрипник, Д. А. Обеспечение безопасности персональных данных : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 121 с. — ISBN 978-5-4497-0334-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS.
7. Хачатрян, Г. А. Организация и технология работы с конфиденциальными документами : учебник для СПО / Г. А. Хачатрян, И. В. Кузнецова. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2020. — 283 с. — ISBN 978-5-4488-0742-8, 978-5-4497-0783-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART.
8. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 с. — ISBN 978-5-4497-0338-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS.

Дополнительные источники:

- 1 Басалова Г.В. Основы криптографии [Электронный ресурс]: учебное пособие/ Басалова Г.В.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.— 282 с.— Режим доступа: <http://www.iprbookshop.ru/89455.html>.— ЭБС «IPRbooks»
- 2 Граничин О.Н. Информационные технологии в управлении [Электронный ресурс]: учебное пособие/ Граничин О.Н., Кияев В.И.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.— 400 с.— Режим доступа: <http://www.iprbookshop.ru/89437.html>.— ЭБС «IPRbooks»
- 3 Кудинов Ю.И. Интеллектуальные информационные системы [Электронный ресурс]: учебное пособие для СПО/ Кудинов Ю.И.— Электрон. текстовые данные.— Липецк, Саратов: Липецкий государственный технический университет, Профобразование, 2020.— 63 с.— Режим доступа: <http://www.iprbookshop.ru/92828.html>.— ЭБС «IPRbooks»

Интернет ресурсы:

1. Единое окно доступа к образовательным ресурсам. Форма доступа: <http://window.edu.ru>.
2. Единая коллекция цифровых образовательных ресурсов. Форма доступа: <http://schoolcollection.edu.ru>.
3. <http://www.mascom.ru/>
4. <http://nelk.ru/>
5. <http://www.laborkomplekt.ru/>
6. <http://pro-spec.ru/>
7. <http://www.bnti.ru>
8. <http://www.inside-zi.ru/>

### **4.3. Общие требования к организации образовательного процесса**

Реализация рабочей программы учебной практики предполагает проведение учебной практики непосредственно в техникуме и/или в организациях на основе прямых договоров, заключаемых между ГБПОУ «Нижегородский промышленно-технологический техникум» и базой практики, куда направляются обучающиеся. В качестве баз практики могут выступать организации, деятельность которых соответствует профилю специальности.

Студенты в период прохождения учебной практики в организациях полностью выполняют задания, предусмотренные программой практики, соблюдают действующие на организациях правила внутреннего трудового распорядка, а также строго соблюдают требования охраны труда и пожарной безопасности.

### **4.4. Кадровое обеспечение образовательного процесса**

Организацию и руководство учебной практикой осуществляют руководители практики от техникума.

Мастера производственного обучения или преподаватели профессионального цикла, осуществляющие руководство учебной практикой обучающихся, должны иметь высшее или среднее профессиональное образование по профилю профессии, проходить обязательную стажировку в профильных организациях не реже 1-го раза в 3 года.



## 5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

**Контроль и оценка** результатов освоения учебной практики осуществляется руководителем практики в процессе проведения учебных занятий, самостоятельного выполнения обучающимися заданий, выполнения практических проверочных работ. В результате освоения учебной практики в рамках профессиональных модулей обучающиеся проходят промежуточную аттестацию в форме зачета.

Результаты обучения учебной практики УП.01 (освоенные практические навыки умения и знания в рамках ВПД)	Формы и методы контроля и оценки результатов обучения)
<b>Имеет практический опыт:</b>	
использования физических средств защиты объекта;	Экспертная оценка наличия практического опыта работы при выполнении заданий
применения физических средств контроля доступа на объект;	
ведения текущей работы исполнителей с конфиденциальной информацией;	
<b>уметь:</b>	
организовывать охрану персонала, территорий, зданий, помещений и продукции организаций;	Экспертная оценка выполненных заданий
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;	
<b>знать:</b>	
виды и способы охраны объекта;	Экспертная оценка
особенности охраны персонала организации;	

основные направления и методы организации режима и охраны объекта;	выполненных заданий, тестирование знаний
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.	

<b>Результаты обучения учебной практики УП.02 (освоенные практические навыки умения и знания в рамках ВПД)</b>	<b>Формы и методы контроля и оценки результатов обучения</b>
<b>иметь практический опыт:</b>	
ведения учета и оформления бумажных и машинных носителей конфиденциальной информации;	Экспертная оценка наличия практического опыта работы при выполнении заданий
работы с информационными системами электронного документооборота;	
<b>уметь:</b>	
использовать в профессиональной деятельности нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;	Экспертная оценка выполненных заданий
разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации;	

документировать ход и результаты служебного расследования;	
определять состав документируемой конфиденциальной информации;	
подготавливать, издавать и учитывать конфиденциальные документы;	
составлять номенклатуру конфиденциальных дел;	
формировать и оформлять конфиденциальные дела;	
организовывать и вести конфиденциальное делопроизводство, в том числе с использованием вычислительной техники;	
использовать системы электронного документооборота;	
<b>знать:</b>	
основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;	Экспертная оценка выполненных заданий, тестирование знаний
правовые основы защиты конфиденциальной информации по видам тайны;	
порядок лицензирования деятельности по технической защите конфиденциальной информации;	
правовые основы деятельности подразделений защиты информации;	
правовую основу допуска и доступа персонала к защищаемым сведениям;	
правовое регулирование взаимоотношений администрации и персонала в области защиты информации;	
систему правовой ответственности за утечку информации и утрату носителей информации;	
правовые нормы в области защиты интеллектуальной собственности;	
порядок отнесения информации к разряду конфиденциальной информации;	
порядок разработки, учета, хранения, размножения и уничтожения конфиденциальных документов;	
организацию конфиденциального документооборота;	
технологии работы с конфиденциальными документами;	
организацию электронного документооборота	

<p align="center"><b>Результаты обучения учебной практики УП.03 (освоенные практические навыки умения и знания в рамках ВПД)</b></p>	<p align="center"><b>Формы и методы контроля и оценки результатов обучения</b></p>
<p><b>иметь практический опыт:</b></p>	
<p>участия в эксплуатации систем и средств защиты информации защищаемых объектов;</p>	<p>Экспертная оценка наличия практического опыта работы при выполнении заданий</p>
<p>применения технических средств защиты информации;</p>	
<p>выявления возможных угроз информационной безопасности объектов защиты;</p>	
<p><b>уметь:</b></p>	
<p>работать с техническими средствами защиты информации;</p>	<p>Экспертная оценка выполненных заданий</p>
<p>работать с защищенными автоматизированными системами;</p>	
<p>передавать информацию по защищенным каналам связи;</p>	
<p>фиксировать отказы в работе средств вычислительной техники;</p>	
<p><b>знать:</b></p>	
<p>виды, источники и носители защищаемой информации;</p>	<p>Экспертная оценка выполненных заданий, тестирование знаний</p>
<p>источники опасных сигналов;</p>	
<p>структуру, классификацию и основные характеристики технических каналов утечки информации;</p>	
<p>классификацию технических разведок и методы противодействия им;</p>	
<p>методы и средства технической защиты информации;</p>	
<p>методы скрытия информации;</p>	
<p>программно-аппаратные средства защиты информации;</p>	
<p>структуру подсистемы безопасности операционных систем и выполняемые ею функции;</p>	
<p>средства защиты в вычислительных сетях;</p>	
<p>средства обеспечения защиты информации в системах управления базами данных;</p>	
<p>критерии защищенности компьютерных систем;</p>	
<p>методики проверки защищенности объектов информатизации на соответствие требованиям нормативных правовых актов.</p>	

<p align="center"><b>Результаты обучения учебной практики УП.04 (освоенные практические навыки умения и знания в рамках ВПД)</b></p>	<p align="center"><b>Формы и методы контроля и оценки результатов обучения</b></p>
<p><b>иметь практический опыт:</b></p>	
<p>подключения кабельной системы персонального компьютера, периферийного и мультимедийного оборудования;</p>	<p>Экспертная оценка наличия практического опыта работы при выполнении заданий</p>
<p>настройки параметров функционирования персонального компьютера, периферийного и мультимедийного оборудования;</p>	
<p>ввода цифровой и аналоговой информации в персональный компьютер с различных носителей, периферийного и мультимедийного оборудования;</p>	
<p>сканирования, обработки и распознавания документов;</p>	
<p>конвертирования медиафайлов в различные форматы, экспорта и импорта файлов в различные программы-редакторы</p>	
<p>обработки аудио-, визуального и мультимедийного контента с помощью специализированных программ-редакторов;</p>	
<p>создания и воспроизведения видеороликов, презентаций, слайд-шоу, медиафайлов и другой итоговой продукции из исходных аудио-визуальных и мультимедийных компонентов;</p>	
<p>осуществления навигации по ресурсам, поиска, ввода и передачи данных с помощью технологий и сервисов сети Интернет;</p>	
<p>управления медиатекой цифровой информации;</p>	
<p>передачи и размещения цифровой информации;</p>	
<p>тиражирования мультимедиа контента на съемных носителях информации;</p>	
<p>осуществления навигации по ресурсам, поиска, ввода и передачи данных с помощью технологий и сервисов сети Интернет;</p>	
<p><b>уметь:</b></p>	
<p>подключать и настраивать параметры функционирования персонального компьютера, периферийного и мультимедийного оборудования;</p>	<p>Экспертная оценка выполненных заданий</p>
<p>настраивать основные компоненты графического интерфейса операционной системы и специализированных программ-редакторов;</p>	
<p>управлять файлами данных на локальных, съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в сети Интернет;</p>	
<p>производить распечатку, копирование и тиражирование документов на принтере и других периферийных устройствах вывода;</p>	
<p>распознавать сканированные текстовые документы с помощью программ распознавания текста;</p>	
<p>вводить цифровую и аналоговую информацию в персональный компьютер с различных носителей, периферийного и мультимедийного оборудования</p>	
<p>создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики;</p>	

конвертировать файлы с цифровой информацией в различные форматы;	
производить сканирование прозрачных и непрозрачных оригиналов;	
производить съемку и передачу цифровых изображений с фото- и видеокамеры на персональный компьютер;	
обрабатывать аудио, визуальный контент и медиафайлы средствами звуковых, графических и видео-редакторов;	
создавать видеоролики, презентации, слайд-шоу, медиафайлы и другую итоговую продукцию из исходных аудио, визуальных и мультимедийных компонентов;	
воспроизводить аудио, визуальный контент и медиафайлы средствами персонального компьютера и мультимедийного оборудования;	
производить распечатку, копирование и тиражирование документов на принтере и других периферийных устройствах вывода;	
использовать мультимедиа-проектор для демонстрации содержимого экранных форм с персонального компьютера;	
вести отчетную и техническую документацию;	
подключать периферийные устройства и мультимедийное оборудование к персональному компьютеру и настраивать режимы их работы;	
создавать и структурировать хранение цифровой информации в медиатеке персональных компьютеров и серверов;	
передавать и размещать цифровую информацию на дисках персонального компьютера, а также дисковых хранилищах локальной и глобальной компьютерной сети;	
тиражировать мультимедиа контент на различных съемных носителях информации;	
осуществлять навигацию по веб-ресурсам Интернета с помощью веб-браузера;	
создавать и обмениваться письмами электронной почты;	
публиковать мультимедиа контент на различных сервисах в сети Интернет;	
осуществлять резервное копирование и восстановление данных;	
осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ;	
осуществлять мероприятия по защите персональных данных;	
<b>знать:</b>	
устройство персональных компьютеров, основные блоки, функции и технические характеристики;	Экспертная оценка выполненных заданий, тестирование знаний
архитектуру, состав, функции и классификацию операционных систем персонального компьютера;	
виды и назначение периферийных устройств, их устройство и принцип действия, интерфейсы подключения и правила эксплуатации;	
принципы установки и настройки основных компонентов операционной системы и драйверов периферийного оборудования;	
принципы цифрового представления звуковой, графической, видео и мультимедийной информации в персональном компьютере;	
виды и параметры форматов аудио-, графических, видео- и мультимедийных файлов и методы их конвертирования;	

назначение, возможности, правила эксплуатации мультимедийного оборудования;	
основные типы интерфейсов для подключения мультимедийного оборудования;	
основные приемы обработки цифровой информации;	
назначение, разновидности и функциональные возможности программ обработки звука;	
назначение, разновидности и функциональные возможности программ обработки графических изображений;	
назначение, разновидности и функциональные возможности программ обработки видео- и мультимедиа контента;	
принципы лицензирования и модели распространения мультимедийного контента;	
нормативные документы по установке, эксплуатации и охране труда при работе с персональным компьютером, периферийным оборудованием и компьютерной оргтехникой;	
структуру, виды информационных ресурсов и основные виды услуг в сети Интернет;	
назначение, разновидности и функциональные возможности программ для создания веб-страниц; нормативные документы по охране труда при работе с персональным компьютером, периферийным., мультимедийным оборудованием и компьютерной оргтехникой	
назначение, разновидности и функциональные возможности программ для публикации мультимедиа контента;	
принципы лицензирования и модели распространения мультимедийного контента;	
нормативные документы по установке, эксплуатации и охране труда при работе с персональным компьютером, периферийным оборудованием и компьютерной оргтехникой;	
структуру, виды информационных ресурсов и основные виды услуг в сети Интернет;	
основные виды угроз информационной безопасности и средства защиты информации: принципы антивирусной защиты персонального компьютера;	
состав мероприятий по защите персональных данных.	