Частное учреждение профессионального образования
«Высшая школа предпринимательства»
(ЧУПО «ВШП»)

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.13 «Основы информационной безопасности»

для специальности среднего профессионального образования:
09.02.07 Информационные системы и программирование

Квалификация базовой подготовки: программист

Форма обучения: очная

Тверь, 2021

ПРИНЯТО

Протокол заседания педагогического
совета ЧУПО «ВШП»
№01 от «13» августа 2021 г.

Разработана на основе Федерального
компонента государственного
стандарта среднего профессионального
образования по специальности 09.02.07
Информационные системы и
программирование
квалификация: программист

УТВЕРЖДАЮ: Директор ЧУПО «ВШП» _____ Аллабян М.Г.

М.П.

Составитель: Соколов Б.А., преподаватель

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

1.1. Область применения программы

Рабочая программа учебной дисциплины «Менеджмент в профессиональной деятельности» является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности 09.02.07 Информационные системы и программирование СПО.

1.2. Место дисциплины в структуре программы подготовки специалистов среднего звена:

Дисциплина ОП.01 Основы информационной безопасности входит в общепрофессиональный цикл, является дисциплиной, дающей начальные представления и понятия в области информационной безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.

1.3. Цель и планируемые результаты освоения дисциплины:

В результате освоения учебной дисциплины обучающийся должен уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации;

В результате освоения учебной дисциплины обучающийся должен знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности;

1.4. Рекомендуемое количество часов на освоение программы учебной дисциплины:

Общий объем образовательной нагрузки — 66 ч.

в том числе:

- Теоретическое обучение — 29 ч.
- Лабораторные и практические занятия — 24 ч.
- Промежуточная аттестация — 1 ч.
- Самостоятельная работа — 12 ч.

2. СТРУКТУРА И СОДЕРЖАНИЕ

2.1. Объем и виды учебной работы

Вид учебной работы	
Общий объем образовательной нагрузки	**66**
в том числе:	
Теоретическое обучение	29
Лабораторные и практические занятия	24
Промежуточная аттестация	1
Самостоятельная работа	12

2.2. Тематический план и содержание

Наименование разделов и тем	**Содержание учебного материала**	**Объем (в часах)**
Тема 1. Основные понятия и задачи информационной безопасности	**Теоретическое обучение**	**8**
	Понятие информации и информационной безопасности.	
	Информация, сообщения, информационные процессы как объекты информационной безопасности.	
	Обзор защищаемых объектов и систем.	
	Понятие «угроза информации».	
	Понятие «риска информационной безопасности».	
	Примеры преступлений в сфере информации и информационных технологий.	
	Сущность функционирования системы защиты информации.	
	Защита человека от опасной информации	
	Лабораторные и практические занятия	**8**
	Целостность, доступность и конфиденциальность информации.	
	Классификация информации по видам тайны и степеням конфиденциальности.	
	Понятия государственной тайны и конфиденциальной информации.	
	Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.	
	Самостоятельная работа	**2**
Тема 2. Основы защиты	**Теоретическое обучение**	**6**

информации	Цели и задачи защиты информации. Основные понятия в области защиты информации.	
	Элементы процесса менеджмента ИБ.	
	Модель интеграции информационной безопасности в основную деятельность организации.	
	Понятие Политики безопасности.	
	Лабораторные и практические занятия	**8**
	Определение объектов защиты на типовом объекте информатизации.	
	Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	
	Самостоятельная работа	**2**
Тема 3. Угрозы безопасности защищаемой информации	**Теоретическое обучение**	**6**
	Понятие угрозы безопасности информации	
	Системная классификация угроз безопасности информации.	
	Каналы и методы несанкционированного доступа к информации	
	Уязвимости. Методы оценки уязвимости информации	
	Протоколы и стеки протоколов	
	Распределение протоколов по назначению в модели OSI	
	Доменные имена, форматы и классы IP- адресов.	
	Подсети и маски подсетей. Система DNS.	
	Лабораторные и практические занятия	**4**
	Практическая работа №1. Определение угроз объекта информатизации и их классификация	
	Самостоятельная работа	**6**
Тема 4. Методологические подходы к защите информации	**Теоретическое обучение**	**9**
	Анализ существующих методик определения требований к защите информации.	
	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.	
	Виды мер и основные принципы защиты информации.	
	Организационная структура системы защиты информации	
	Законодательные акты в области защиты информации.	
	Российские и международные стандарты, определяющие требования к защите информации.	
	Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации	
	Лабораторные и практические занятия	**4**

	Практическая работа №2. Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	
	Самостоятельная работа	**2**
	Промежуточная аттестация	**1**
	Общий объем образовательной нагрузки	**66**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия отдельного учебного кабинета.

Оборудование учебного кабинета:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- меловая или маркерная доска

Технические средства обучения:

- компьютеры с доступом в интернет и соответствующим ПО
    - Microsoft Windows 10 Pro
    - Google Chrome
    - Microsoft Office 2019
- мультимедиа-проектор и экран для проецирования изображения

3.2. Информационное обеспечение обучения

Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

- Мельников В.П., Куприянов А.И. Информационная безопасность:учебник / под ред. В.П. Мельникова. — М.: КНОРУС, 2021.
- Родичев Ю. Информационная безопасность, Национальные стандарты Российской Федерации, 2-е издание, учебное пособие, СПБ: Питер, 2019.

Дополнительные источники:

- Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. — М.: Издательство КДУ, 2019. https://znanium.com/catalog/product/987215
- Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD): учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — 2-е изд., стер. — М. : КНОРУС, 2017. http://znanium.com/catalog/product/763644
- Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. — М.: Инфа-М. 2018. https://znanium.com/catalog/product/957144
- Бубнов А.А., Пржегорлинский В. Н., Савинкин О. А., Основы информационной безопасности (2-е изд.), М. Академия, 2019. https://academia-library.ru/catalogue/4831/411969/
- Бондарев В.В. Введение в информационную безопасность автоматизированных систем. Учебное пособие. — М.: МГТУ им. Баумана, 2018. http://biblioclub.ru/index.php?page=book&id=571750

Интернет-ресурсы:

- Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/
- Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

- Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
- Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
- Справочно-правовая система «Консультант Плюс» www.consultant.ru
- Справочно-правовая система «Гарант» » www.garant.ru
- Федеральный портал «Российское образование www.edu.ru
- Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
- Российский биометрический портал www.biometrics.ru
- Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\: www.ict.edu.ru
- Сайт Научной электронной библиотеки www.elibrary.ru

Профессиональные базы данных и справочные системы:

- Федеральная служба государственной статистики https://rosstat.gov.ru/
- Наукометрическая и реферативная база данных SCOPUS https://www.scopus.com
- Информационно-справочная система "КонсультантПлюс"

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения теоретических и практических занятий, тестирования, устного опроса, а также выполнения обучающимися индивидуальных заданий, проектов, исследований, презентаций, докладов, сообщений.
Образовательное учреждение, реализующее подготовку по учебной дисциплине, обеспечивает организацию и проведение промежуточной аттестации и текущего контроля индивидуальных образовательных достижений — демонстрируемых обучающимися знаний, умений и навыков.
Текущий контроль проводится преподавателем в процессе проведения практических занятий, тестирования, устного опроса, а также выполнения обучающимися индивидуальных заданий, самостоятельных и контрольных работ.

Для промежуточной аттестации и текущего контроля образовательными учреждениями создаются фонды оценочных средств (ФОС).

Обучение завершается промежуточной аттестацией в форме **зачета**.

Перечень умений, осваиваемых в рамках дисциплины:
- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации;

Перечень знаний, осваиваемых в рамках дисциплины:
- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности;

Методы оценки
- устный опрос,
- тестирование,
- самостоятельная работа,
- выполнение индивидуальных заданий различной сложности,
- оценка ответов в ходе эвристической беседы,
- подготовка презентаций