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

Рабочая программа учебной дисциплины

ОП.06 Основы информационной безопасности

специальность 10.02.01 Организация и технология защиты информации

Нижний Новгород

2021 г.

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности (специальностям) среднего профессионального образования (далее СПО) 10.02.01 Организация и технология защиты информации, входящей в укрупненную группу 10.00.00 Информационная безопасность

Организация-разработчик:
ГБПОУ «Нижегородский промышленно- технологический техникум»

СОДЕРЖАНИЕ

Стр.

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины «Основы информационной безопасности» является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.01 Организация и технология защиты информации.

1.2. Место профессионального модуля в структуре основной профессиональной образовательной программы

Учебная дисциплина ОП.06 Основы информационной безопасности входит в ОП.00 Общепрофессиональные дисциплины.

1.3. Цель, задачи профессионального модуля, требования к результатам освоения дисциплины:

Целью изучения учебной дисциплины является развитие делового и логического мышления студентов, приобретение навыков организации работы персонала с конфиденциальной информацией.

Задачи:

1. изучить сущность и понятие информационной безопасности, характеристику ее составляющих, понятие «угроза информации», рассмотреть классификацию информации по видам тайны и степеням конфиденциальности, жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи, особенности и принципы приема (перевода) сотрудников на работу, связанную с владением конфиденциальной информацией, особенности проведения собеседования, анкетирования, тестирования и опроса, структуру разрешительной системы, понятие доступа, правовую ответственность персонала за разглашение конфиденциальной информации.
2. научиться классифицировать персонал по степени их владения

тайной фирмы и объемам известной им конфиденциальной 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.

3. формировать общие и профессиональные компетенции.

В результате изучения профессионального модуля обучающийся должен:

уметь:

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

- применять основные правила и документы системы сертификации Российской Федерации;

- классифицировать основные угрозы безопасности информации;

знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;

- место информационной безопасности в системе национальной безопасности страны;

- источники угроз информационной безопасности и меры по их предотвращению;

- жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;

- современные средства и способы обеспечения информационной безопасности;

В процессе освоения дисциплины у обучающегося должны формироваться общие и профессиональные компетенции.

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 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.

ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий.

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.

Личностные результаты реализации программы воспитания *(дескрипторы)*	**Код личностных результатов**

	реализации программы воспитания
Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации	**ЛР 13**
Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм	**ЛР 14**
Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности.	**ЛР 15**

1.4. Рабочее количество часов на освоение программы профессионального модуля:

максимальной учебной нагрузки обучающегося 120 часов, включая:

обязательной аудиторной учебной нагрузки обучающегося 80 часа,

в том числе:

лабораторных и практических занятий – 40 часов;

самостоятельной работы обучающегося – 40 часов.

Промежуточная аттестация проводится в форме: экзамена

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Основы информационной безопасности

Наименования учебной дисциплины	Всего часов	Объем времени, отведенный на освоение учебной дисциплины				
		Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося	
		Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов
1	2	3	4	5	6	7
Основы информационной безопасности	120	80	40		40	
Всего:	120	80	40		40	

2.2. Содержание обучения по учебной дисциплине

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся		Объем часов	ЛР, ОК, ПК
1	**2**		**3**	
Раздел 1. Теоретические основы информационной безопасности				ЛР13-15, ОК 1 - 5, 8, 9 ПК 1.6, 3.1 - 3.4
Тема 1 Политика и концепции информационной безопасности	**Содержание учебного материала**		**10**	
	1	Понятие информации как объекта защиты. Основные составляющие информационной безопасности.	2	
	2	Понятие и концепции информационной войны	2	
	3	Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.	2	
	4	Защищаемая информация. Степени конфиденциальности. Виды тайн.	2	
	5	Жизненные циклы конфиденциальной информации в процессе ее создания, обработки и передачи	2	
Тема 2 Уязвимость информации в информационных системах	**Содержание учебного материала**		**12**	
	6	Виды и формы проявления уязвимости информации.		
	7	Классификация атак на информационные системы	2	
	8	Источники угроз ИБ и меры по их предотвращению	2	
	9	Каналы и методы НСД к защищаемой информации	2	
	10	Носители защищаемой информации. Объекты. Виды.	2	

	11	Классификация компьютерных вирусов	2	
Раздел 2. Методология защиты информации				ЛР13-15, ОК 1 - 5, 8, 9 ПК 1.6, 3.1 - 3.4
Тема 3 Защита информации	**Содержание учебного материала**		**6**	
	12	Система сертификации и лицензирования.	2	
	13	Центр безопасности Windows.	2	
	14	Межсетевой экран	2	
	Практические работы		**8**	
	1	Проверка компьютера на предмет наличия уязвимостей	2	
	2	Восстановление зараженных файлов	2	
	3	Защита и восстановление данных, используя систему архивации	2	
	4	Настройка «антивируса Касперского»	2	
	Содержание учебного материала		**6**	
	15	Методологические подходы к защите информации и принципы ее организации	2	
	16	Защита информации средствами разграничения прав доступа	2	
	17	Особенности обеспечения защиты информации в локальных и корпоративных сетях.	2	
	Практические работы		**12**	
	5	Порядок сертификации информационных продуктов.	2	
	6	Порядок лицензирования деятельности в информационной сфере.	2	
	7	Настройка безопасности почтового клиента	2	

	8	Настройка и использование межсетевого экрана в MS Windows	2	
	9	Разграничения прав доступа	2	
	10	Использование брандмауэра для анализа межсетевого трафика	2	
	Содержание учебного материала		**2**	
	18	Криптографические методы защиты информации	2	
	Практические работы		**12**	
	11	Криптографическое преобразования.	4	
	12	Управление криптографическими ключами.	4	
	13	Электронная цифровая подпись (ЭЦП)	4	
	Содержание учебного материала		**2**	
	19.	Шифрование файлов и дисков	2	
	Практические работы		**4**	
	14	Шифрование файлов EFS	2	
	15	Шифрование дисков	2	
	Содержание учебного материала		**2**	
	20.	Реестр Windows.	2	
	Практические работы		**4**	
	16	Исследование реестра на предмет возможных уязвимостей и вирусов	4	
	Самостоятельная работа обучающихся Выдающиеся личности в истории вычислительной техники. Общество в период развития информатизации. Понятие государственной тайны. Отличия функциональных требований от требований доверия		40	

	Механизмы безопасности используемые для обеспечения конфиденциальности трафика. Категории государственных информационных ресурсов. Ответственность за использование и распространение вредоносных программ для ЭВМ. Механизм обеспечения ИБ в вычислительных сетях. Особенность компьютерного вируса «Чернобыль». Хронология развития компьютерных вирусов. История криптографической деятельности. Простейшие шифры и их свойства. Ключевые системы разграничения доступа и электронная цифровая связь. Методы и средства ограничения доступа к компонентам ЭВМ. Системы опознавания нарушителей. Автоматизация технического контроля защиты потоков информации. Защита процессов переработки информации в СУБД. Отечественное нормативно-правовое обеспечение ИБ. Технологии предотвращения угроз ИБ. Модели защиты при отказе в обслуживании. Области и сферы обеспечения ИБ.		
	Всего:	**120**	
	Теоретические занятия	**40**	
	Практические работы	**40**	
	Самостоятельная работа	**40**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к материально-техническому обеспечению

Оборудование учебного кабинета и рабочих мест кабинета:

- рабочее место преподавателя;
- рабочие места по количеству обучающихся;
- комплекты учебно-методической документации;
- наглядные пособия.

Технические средства обучения:

- мультимедийный проектор;
- интерактивная доска;
- компьютеры.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых 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.

Дополнительные источники:

отсутствуют

Интернет-источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru

7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/

8. Российский биометрический портал www.biometrics.ru

9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

10. Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
В результате освоения дисциплины обучающийся должен знать:	
- сущность и понятие информационной безопасности, характеристику ее составляющих;	Экспертная оценка защиты практических работ; экспертная оценка защиты самостоятельных работ.
- место информационной безопасности в системе национальной безопасности страны;	
- источники угроз информационной безопасности и меры по их предотвращению;	
- жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;	
- современные средства и способы обеспечения информационной безопасности.	
В результате освоения дисциплины обучающийся должен уметь:	
- классифицировать защищаемую информацию по видам и степеням конфиденциальности;	Экспертная оценка защиты практических работ; экспертная оценка защиты самостоятельных работ.
- применять основные правила и документы системы сертификации Российской Федерации;	
- Классифицировать основные угрозы безопасности информации.	

Промежуточная аттестация проводится в форме: экзамена