ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МОСКОВСКОЙ ОБЛАСТИ
«ДМИТРОВСКИЙ ТЕХНИКУМ»

ОДОБРЕНО
на заседании ПЦК
физико-математических дисциплин
_____/Л.А. Алешина
«30» августа 2021 г.

Протокол № 1

УТВЕРЖДАЮ
Зам. директора по УМР
_____/Н. Е. Горюшкина /
___»_____ 202_г.

Александровская И.Л.
я подтверждаю этот документ своей удостоверяющей подписью
место подписания
2021.11.08 10:08:45+03'00'

РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.06 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по специальности **10.02.01 Организация и технология защиты информации**

г. Дмитров 2021 г.

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МОСКОВСКОЙ ОБЛАСТИ
«ДМИТРОВСКИЙ ТЕХНИКУМ»

ОДОБРЕНО
на заседании ПЦК
физико-математических дисциплин
_____/Л.А. Алешина
«___» _____ 202_ г.

Протокол №_____

УТВЕРЖДАЮ
Зам. директора по УМР
_____ /Н. Е. Горюшкина /
___»_____ 202_г.

РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.06 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по специальности **10.02.01 Организация и технология защиты информации**

г. Дмитров 2021 г.

Программа учебной дисциплины *ОП.06 Основы информационной безопасности* разработана в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности *10.02.01 Организация и технология защиты информации*, утвержденного приказом Министерства образования и науки Российской Федерации *№ 805 от 28 июля 2014 года (с изменениями и дополнениями)* и зарегистрированного Министерством юстиции Российской Федерации *21 августа 2014 года* (*регистрационный № 33750), с* учетом запросов работодателей на дополнительные результаты освоения образовательной программы подготовки специалистов среднего звена, не предусмотренных ФГОС СПО.

Организация-разработчик:

Государственное бюджетное профессиональное образовательное учреждение Московской области «Дмитровский техникум»

Разработчик:

Белоусов Александр Георгиевич, преподаватель ГБПОУ МО «Дмитровский техникум»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. **Область применения программы**

Программа учебной дисциплины является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.01 Организация и технология защиты информации

1.2. Место дисциплины в структуре основной профессиональной образовательной программы: Учебная дисциплина «Основы информационной безопасности» относится к профессиональному учебному циклу основной профессиональной образовательной программы.

1.3. Цель и планируемые результаты освоения дисциплины:

Цель учебной дисциплины освоить следующие общие компетенции и профессиональные компетенции:

Код ПК, ОК	Умения	Знания
ОК 01-05,08,09 ПК 1.6, 3.1,3.4,	- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - применять основные правила и документы системы сертификации Российской Федерации; - классифицировать основные угрозы безопасности информации	- сущность и понятие информационной безопасности; - место информационной безопасности в системе национальной безопасности страны; - источники угроз информационной безопасности и меры по их предотвращению; - жизненные циклы конфиденциальной информации в процессе её создания, обработки, передачи; - современные средства и способы обеспечения информационной безопасности

1.4. Количество часов на освоение программы дисциплины:

Объем образовательной нагрузки обучающегося 125 часов;
Нагрузка во взаимодействии с преподавателем 83 часа;
Самостоятельная работа обучающегося 42 часа;
Консультации нет
Промежуточная аттестация – экзамен

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объём в часах
Объем образовательной нагрузки	**125**
Нагрузка во взаимодействии с преподавателем	**83**
в том числе:	
лекции, уроки	**36**
практические занятия	**47**
Самостоятельная работа	**42**
Консультации	**не предусмотрены**
Промежуточная аттестация в форме экзамена	

2.1 Тематический план и содержание учебной дисциплины ОП.6 Основы информационной безопасности

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа обучающегося	Объем часов	Уровень освоения
1	2		
Тема 1. Защита информации. Основные понятия и определения	Информационные ресурсы и документирование информации Безопасность информационных ресурсов. Государственные информационные ресурсы. Персональные данные о гражданах. Права на доступ к информации. Вычислительные сети и защита информации. Нормативно-правовая база функционирования систем защиты информации. Компьютерные преступления и особенности их расследования. Промышленный шпионаж и законодательство, правовая защита программного обеспечения авторским правом.	**10**	2
	Практические работы: Уточнение задач информационной безопасности организации. Изучение источников, рисков и форм атак на информации		
	Самостоятельная работа: Предпосылки становления предметной области информационной безопасности. Подготовка к практической работе Подготовка сообщений		
Тема 2. Изучение источников, рисков и форм атак на информацию в ИС, вредоносных программ и компьютерных вирусов. Проблемы защиты информации в ИС	Изучение источников, рисков и форм атак на информацию в ИС, вредоносных программ и компьютерных вирусов. Проблемы защиты информации в ИС. Классификация угроз и меры по обеспечению сохранности информации в ИС. Классификация рисков и основные задачи обеспечения безопасности информации в ИС. Защита локальных сетей и операционных систем. Интеграция систем защиты. Internet в структуре информационно-аналитического обеспечения ИС и угрозы исходящие от использования «электронной почты».	**8**	2
	Практические работы: Изучение источников, рисков и форм атак на информацию в АСОИУ. Классификация рисков и основные задачи обеспечения безопасности информации в АСОИУ		
	Самостоятельная работа: Математические модели систем и процессов защиты информации. Подготовка сообщений Подготовка к практической работе		
Тема 3. Законодательные и правовые основы защиты компьютерной информации	Законодательная, нормативно-методическая и научная база систем защиты информации. Требования к содержанию нормативно-методических документов по защите информации. Российское законодательство по защите информационных технологий. Политика безопасности. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС.	**8**	2

информационных технологий. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС	**Практические работы:** Изучение Российского законодательства по защите информационных технологий. Изучение нормативно-правовой информации		
	Самостоятельная работа: Международное и российское законодательство в сфере информационной безопасности Подготовка сообщений Подготовка к практической работе		
Тема 4. Международные и Государственные стандарты информационной безопасности и их использование в практической деятельности	Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Доктрина информационной безопасности Российской Федерации. Классификация защищенности средств вычислительной техники. Международные стандарты по защите информации. Стандарты безопасности в Интернете.	**20**	2
	Практические работы: Изучение международных и государственных стандартов информационной безопасности		
	Самостоятельная работа: Подготовка сообщений Подготовка к практической работе		
Тема 5. Криптографические модели. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в ИС	Криптографические модели. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в ИС. Режим простой замены. Режим гаммирования. Режим гаммирования с обратной связью. Режим выработки имитовставки. Блочные и поточные шифры. Методы генерации псевдослучайных последовательностей чисел.	**20**	2
	Практические работы: Изучение симметричных и ассиметричных криптосистем для защиты компьютерной информации в АСОИУ		
	Самостоятельная работа: Подготовка сообщений Подготовка к практической работе		
Тема 6. Стандартные алгоритмы шифрования. Безопасность и быстродействие криптосистем	Стандартные алгоритмы шифрования. Основные понятия и определения. Шифры перестановки. Шифрующие таблицы. Применение магических квадратов, Концепция криптосистемы с открытым ключом. Криптосистема шифрования данных К5А Безопасность и быстродействие криптосистемы К5А, Изучение американского стандарта шифрования данных ОЕ5. Основные режимы работы алгоритма ВЕ5. Отечественный стандарт шифрования данных.	**20**	2
	Практические работы: Изучение стандартных алгоритмов шифрования. Безопасность и быстродействие криптосистем		

	Самостоятельная работа: Подготовка к практической работе Подготовка сообщений		
Тема 7. Методы идентификации и проверки подлинности пользователей компьютерных систем	Основные понятия и концепции идентификации и проверки подлинности пользователей компьютерных систем. Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверка подлинности пользователей. Протоколы идентификации с нулевой передачей знаний. Проблема аутентификации данных и электронная цифровая подпись. Алгоритмы цифровой подписи. Отечественный стандарт цифровой подписи. Биометрические средства идентификации пользователей.	**10**	2
	Практические работы: Изучение принципов идентификации и механизмов подтверждения подлинности пользователя. Правила формирования электронной цифровой подписи		
	Самостоятельная работа: Подготовка сообщений Подготовка к практической работе		
Тема 8. Многоуровневая защита корпоративных сетей. Защита компьютерных систем от удаленных атак через сеть Internet	Многоуровневая защита корпоративных сетей. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты информации. Защита компьютерных систем от удаленных атак через сеть Intrnet.	**20**	2
	Практические работы: Изучение средств защиты локальных сетей от несанкционированного доступа. Анализ функционирования маршрутизаторов, шлюзов сетевого уровня и межсетевых экранов.		
	Самостоятельная работа: Подготовка сообщений Подготовка к практической работе		
Тема 9. Защита информации в компьютерных сетях, антивирусная защита	Классификация способов защиты информации в компьютерных сетях. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействия. Защита от разрушающих программных воздействий. Антивирусная защита в сетях. Понятие изолированной программной среды. Рекомендации по защите информации Internet.	**19**	2
	Практические работы: Анализ способов защиты информации в компьютерных сетях от разрушающего программного воздействия. Изучение методов борьбы с компьютерными вирусами и средств защиты информации в Internet. Угрозы исходящие от использования " электронной почты"		

	Самостоятельная работа: Защита информационной инфраструктуры от атак. Подготовка к практической работе		
Тема 10. Требования к системам информационной защиты ИС	Организационные требования к системам информационной защиты ИС. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению. Требования по применению способов, методов и средств защиты информации. Требования к документированию событий в системе и выявлению несанкционированного доступа. Организация аудита информационной безопасности ИС и предприятия в целом		2
	Самостоятельная работа: Комплексная защита информационной инфраструктуры и ресурсов. Оценка эффективности СЗИ Подготовка к зачёту		
Итого:		**83**	
Самостоятельная работа:		**42**	
Всего:		**125**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ РАБОЧЕЙ ДИСЦИПЛИНЫ

3.1. Образовательные технологии

Технологии обучения выбираются таким образом, чтобы учитывать индивидуальные коммуникационные и учебные способности обучающихся и способствовать их социальной и профессиональной адаптации. В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

В качестве образовательных технологий, используемых при реализации различных видов учебной работы и дающих наиболее эффективные результаты освоения данной адаптационной дисциплины, применяются:

– Лекционно-семинарская система – дает возможность сконцентрировать материал в блоки и преподносить его как единое целое, а контроль проводить по предварительной подготовке обучающихся.

– Информационно-коммуникационные технологии – дают возможность преподавателю визуализировать процесс усвоения учебного материала обучающимися, используя интеграцию в одном программном продукте разнообразных видов информации; предоставляют удобные возможности работы с материалом за счет нелинейной организации контента (выделения ключевых объектов и организации перекрестных ссылок между ними).

– Технология обучения в малых группах – предполагает организацию групп обучающихся, работающих совместно над решением какой-либо проблемы, служит прекрасной подготовкой к проектной деятельности обучающихся.

– Игровая технология – способствует развитию познавательных интересов, активизации деятельности учащихся, установлению коммуникативных связей.

– Технология проблемного обучения. Особенность проблемных методов состоит в том, что методы основаны на создании проблемных ситуаций, активной познавательной деятельности обучающихся, состоящих в поиске и решении сложных вопросов, требующих актуализации знаний, анализа.

Активные и интерактивные формы проведения занятий, используемые в учебном процессе

Семестр	**Вид занятия***	**Используемые активные и интерактивные формы проведения занятий**	**Разработанные учебно-методические материалы, обеспечивающие реализацию формы проведения занятий**
6	Л	Круглый стол, проблемная лекция	Тематические презентации, электронные образовательные ресурсы, опорные конспекты лекций
	ПЗ, С	Творческие задания, работа в малых группах;	Презентации, контекстные кейсы в электронном виде, практические задания, метод кейсов, деловая игра

*) Л-лекция, ПЗ – практические занятия, С – семинары

3.2. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения: лаборатория технических средств обучения

ОП.06 Основы информационной безопасности	Лаборатория технических средств обучения учебная Аудитория для проведения занятий всех видов, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Кабинет: - доска классная - стол преподавателя - кресло для преподавателя - столы ученические - кресла с регулируемой высотой - класс ПК, объединённых в локальную сеть, с выходом на эл.портал техникума - проектор - демонстрационные наглядные пособия	Microsoft Windows , Microsoft Office, Google Chrome , Kaspersky Endpoint Security Microsoft Visual Studio iTALC , Microsoft Visio AnyLogic ArgoUML ARIS EXPRESS Erwin Inkscape Maxima Microsoft SQL Server Management Studio MPLAB Notepad++ Oracle VM Virtual Box Paint .NET SciLab WinAsm GNS3 Информационно-справочная система «Консультант – плюс» NanoCAD
	Библиотека, читальный зал (специализированный кабинет) с выходом в сеть Интернет.	Аудитория: - комплекты учебной мебели; -компьютерная техника с подключением к сети «Интернет», доступом в электронную информационно-образовательную среду и электронно-библиотечную систему.	Microsoft Windows , MicrosoftOffice, GoogleChrome , Kaspersky Endpoint Security
	Помещения для самостоятельной работы и курсового проектирования,	Кабинет: - комплекты учебной мебели; -компьютерная техника с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду.	Microsoft Windows , MicrosoftOffice, GoogleChrome , KasperskyEndpointSecurity. Информационно-справочная система «Консультант – плюс»
		Аудитория : - комплекты учебной мебели; - компьютерная техника с подключением к сети «Интернет», доступом в электронную информационно-образовательную среду и электронно-библиотечную систему.	Microsoft Windows , MicrosoftOffice, GoogleChrome , Kaspersky Endpoint Security

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд Дмитровского техникума имеет печатные и/или электронные образовательные и информационные ресурсы.

3.2.1 Основные источники

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2016. — 136 с.
2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.
3. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 с.
4. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ-ДАНА, 2016. — 239 с.
5. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ, 2016. — 239 с.
6. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2017. — 536 с.
7. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.

3.2.2 Дополнительные источники

1. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.
2. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2016. — 432 с.
3. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА, 2016. — 296 с.
4. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2017. — 277 с.
5. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 с.

3.3.3. Интернет ресурсы:

1. Образовательная платфора «Юрайт» https://urait.ru/news/1064IP
2. СПО в ЭБС Знаниум https://new.znanium.com/collections/basic IP.31.44.94.39
3. ЭОС «Русское слово» Электронные формы учебников, рабочие тетради, пособия и интерактивные тренажеры https://forms.yandex.ru/u/5e6f667c2f089d0b3be3ed6a/ **IP адрес: 93.158.134.22** . Подробнее на сайте: https://xn—-dtbhthpdbkkaet.xn–p1ai/articles/81165/ **IP адрес: 193.124.206.248**
4. Электронная библиотека Издательского центра «Академия» https://academia-library.ru/
5. Система электронного обучения «Академия-Медиа 3.5» https://elearning.academia-moscow.ru/
6. Интернет-портал московского среднего профессионального образования https://spo.mosmetod.ru/IP.195.9.186.84
7. Образовательные ресурсы Академия Ворлдкиллс Россия https://worldskillsacademy.ru/#/programs IP: 82.146.50.206

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения	***Критерии оценки***	***Формы и методы оценки***
Перечень знаний, осваиваемых в рамках дисциплины: - сущность и понятие информационной безопасности; - место информационной безопасности в системе национальной безопасности страны; - источники угроз информационной безопасности и меры по их предотвращению; - жизненные циклы конфиденциальной информации в процессе её создания, обработки, передачи; - современные средства и способы обеспечения информационной безопасности	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Оценка в рамках текущего контроля результатов выполнения индивидуальных контрольных заданий, результатов выполнения практических работ, устный индивидуальный опрос. Письменный опрос в форме тестирования