МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Колледж

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
МДК.01.04. АНТИВИРУСНЫЕ СИСТЕМЫ

по программе подготовки специалистов среднего звена (ППССЗ) среднего профессионального образования

Специальность:	*10.02.05.Обеспечение информационной безопасности автоматизированных систем*
Обучение:	*по программе базовой подготовки*
Уровень образования, на базе которого осваивается ППССЗ:	*среднее общее образование*
Квалификация:	*техник по защите информации*
Форма обучения:	*очная*

Махачкала - 2021

Рабочая программа дисциплины «Антивирусная система» разработана на основе требований Федерального государственного образовательного стандарта (ФГОС) среднего профессионального образования (СПО) по специальности 10.02.05. Обеспечение информационной безопасности автоматизированных систем от 9 декабря 2016 г. № 1553 для реализации основной профессиональной образовательной программы СПО на базе основного общего образования с получением среднего общего образования.

Организация-разработчик: колледж федерального государственного бюджетного образовательного учреждение высшего образования «Дагестанский государственный университет» (Колледж ДГУ)

Разработчики:

Шахбанова М.И. - преподаватель кафедры естественнонаучных и гуманитарных дисциплин Колледжа ДГУ ВО «Дагестанский государственный университет»
Шахбанова З.И. - доцент, к.э.н. преподаватель кафедры естественнонаучных и гуманитарных дисциплин Колледжа ДГУ ВО «Дагестанский государственный университет»

Рабочая программа дисциплины одобрена на заседании кафедры специальных дисциплин Колледжа ДГУ
протокол №__7__от «27» ___02_____2021г.

Зав. кафедрой_____/Магомедова А.М./

Рабочая программа дисциплины согласована с учебно-методическим управлением «16» ___03_____2021г.

Начальник УМУ, д.б.н., проф. _____ Гасангаджиева А.Г.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Антивирусные системы

1.1. Область применения программы

Рабочая программа дисциплины «Антивирусные системы» является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.05. Обеспечение информационной безопасности автоматизированных систем для очного обучения студентов, имеющих основное общее4 образование, по программе базовой подготовки.
Рабочие программы дисциплин, адаптированные для обучения лиц с ограниченными возможностями здоровья, разрабатываются с учетом конкретных ограничений здоровья лиц, зачисленных в колледж, и утверждаются в установленном порядке.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина «Антивирусные системы» относится к профессиональному модулю «Эксплуатация автоматизированных систем в защищенном исполнении» профессионального цикла ПССЗ.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины:

Содержание программы учебной дисциплины «Антивирусные системы» направлено на достижение следующей **цели:**

- обзор современных проблем в сфере информационной безопасности в информационных системах, а также обзор направлений развития программы информационной безопасности России;
- рассмотреть методы защиты информации, выработать практические навыки работы с антивирусными программами, научиться сравнивать антивирусные программные продукты;

Задачи дисциплины:

- применение антивирусных средств защиты;
- методы и средства защиты информации от несанкционированного доступа сформировать навыки работы в глобальной сети;
- рассмотреть основные методики и подходы обеспечения информационной безопасности в рамках современных автоматизированных систем.
- раскрыть принципы построения защищенных информационных систем и поддержания подсистемы защиты информации в актуальном состоянии.
- показать особенности реализации общих методик защиты информации на различных платформах.

Освоение содержания учебной дисциплины «Антивирусные системы» обеспечивает достижение студентами следующих результатов:

Общие компетенции

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

Профессиональные компетенции

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

В результате освоения дисциплины обучающийся должен уметь:

Обучающийся должен:

Уметь:

- организовывать антивирусную защиту информационной системы с помощью антивирусного программного обеспечения;
- обнаруживать, анализировать и удалять компьютерные вирусы и другие вредоносные программы;
- организовать антивирусную защиту информационной системы с помощью антивирусного программного обеспечения.

В результате освоения дисциплины обучающийся должен знать:

Знать:

- методы защиты от компьютерных вирусов;
- принципы разработки и применения антивирусного программного обеспечения;
- методы проникновения вирусов в систему;
- способы их маскировки и воспроизведения;
- сущность предмета компьютерной вирусологии.

При реализации содержания учебной дисциплины «Антивирусные системы» в пределах освоения ОПОП СПО на базе основного общего образования с получением среднего общего образования учебная нагрузка студентов составляет - 112 часов, из них аудиторная (обязательная) учебная нагрузка, включая лекционные и практические занятия- 92 часа; внеаудиторная самостоятельная работа студентов - 20 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	*112*
Обязательная аудиторная учебная нагрузка (всего)	*92*
в том числе:	
теоретическое обучение	*32*
лабораторные работы	-
практические занятия (в т.ч. практическая подготовка)	*60*
контрольные работы	
курсовой проект	
консультации	
Самостоятельная работа обучающегося (всего)	*20*
в том числе:	
самостоятельная работа над курсовым проектом	
внеаудиторная самостоятельная работа	
Промежуточная аттестация в форме дифференцированного зачета	

2.2. **Тематический план и содержание дисциплины** *« Антивирусная система»*

Наименование разделов и тем	**Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работ (проект)** *(если предусмотрены)*	**Объем часов**
1	**2**	**3**
Раздел 1. Методы защиты от вирусов и других вредоносных программных объектов		
Тема 1.1 Классификация компьютерных вирусов	**Содержание учебного материала**	**8**
	Типы вредоносных программ. Общее определение компьютерного вируса Различные типы вирусов Файловые вирусы Загрузочные вирусы Файлово-загрузочные вирусы Стелс-вирусы Шифрующиеся вирусы Полиморфные вирусы Макрокомандные вирусы Почтовые вирусы Вирусы в пакетных файлах ОС Вирусы в драйверах ОС Бестелесные вирусы Вирусы для пиринговых сетей Комбинированные вирусы Известные и неизвестные вирусы Коллекционные вирусы	*2*
	Практические занятия/ Лабораторные занятия	*4*

	1. Типы вредоносных программ. 2. Общее определение компьютерного вируса 3. Различные типы вирусов 4. Файловые вирусы 5. Загрузочные вирусы 6. Файлово-загрузочные вирусы 7. Стелс-вирусы 8. Шифрующиеся вирусы 9. Полиморфные вирусы 10.Макрокомандные вирусы 11.Почтовые вирусы 12.Вирусы в пакетных файлах ОС 13.Вирусы в драйверах ОС 14.Бестелесные вирусы 15.Вирусы для пиринговых сетей 16.Комбинированные вирусы 17.Известные и неизвестные вирусы 18.Коллекционные вирусы	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*2*
Тема 1.2 Классификация других вредоносных программ	**Содержание учебного материала**	**8**
	Логические бомбы Троянские объекты Троянские программы Троянские Web-сайты Троянские сообщения E-Mail Программы Backdoor Средства для получения несанкционированного доступа Техника Phishing Программы Spyware	*2*

	Программы Adware Клавиатурный шпион Комбинированные вредоносные программы	
	Практические занятия/ Лабораторные занятия	*4*
	1. Логические бомбы 2. Троянские объекты 3. Троянские программы 4. Троянские Web-сайты 5. Троянские сообщения E-Mail 6. Программы Backdoor 7. Средства для получения несанкционированного доступа 8. Техника Phishing 9. Программы Spyware 10. Программы Adware 11. Клавиатурный шпион 12. Комбинированные вредоносные программы	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*2*
Тема 1.3. Способы распространения вредоносных программ	**Содержание учебного материала**	**7**
	Файлы исполняемых программ Файлы офисных документов Файлы интерпретируемых программ Загрузочные секторы дисков и дискет Сообщения электронной почты Файлообменные (пиринговые) сети	*2*
	Практические занятия/ Лабораторные занятия. 1. Файлы исполняемых программ 2. Файлы офисных документов 3. Файлы интерпретируемых программ	*4*

	4. Загрузочные секторы дисков и дискет 5. Сообщения электронной почты 6. Файлообменные (пиринговые) сети	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос. Подготовка доклада.	*1*
Тема 1.4. Вредоносное воздействие компьютерных вирусов	**Содержание учебного материала**	**8**
	Визуальные и звуковые эффекты Воздействие на файлы Изменение содержимого секторов диска Воздействие на базы данных Воздействие на аппаратное обеспечение компьютеров Воздействие на систему в целом Получение несанкционированного доступа и похищение информации Компрометация пользователя Социальный инжиниринг	*2*
	Практические занятия/ Лабораторные занятия: 1. Визуальные и звуковые эффекты 2. Воздействие на файлы 3. Изменение содержимого секторов диска 4. Воздействие на базы данных 5. Воздействие на аппаратное обеспечение компьютеров 6. Воздействие на систему в целом 7. Получение несанкционированного доступа и похищении информации 8. Компрометация пользователя 9. Социальный инжиниринг	*4*
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос	*2*
Тема 1.5.	**Содержание учебного материала**	**7**

Обнаружение компьютерных вирусов и других вредоносных программ	Сканирование Эвристический анализ Обнаружение изменений Анализ сетевого трафика Анализ баз данных почтовых программ Обнаружение вирусов в системе автоматизации документооборота Вакцинирование	*2*
	Практические занятия/ Лабораторные занятия: 1. Сканирование 2. Эвристический анализ 3. Обнаружение изменений 4. Анализ сетевого трафика 5. Анализ баз данных почтовых программ 6. Обнаружение вирусов в системе автоматизации документооборота 7. Вакцинирование	*4*
	Консультации	
	Самостоятельная работа обучающихся: Доклад, разработка презентации к докладу на семинаре, поиск информации в сетях.	*1*
Тема 1.6. Типы антивирусных программ	**Содержание учебного материала**	**14**
	Сканеры Сканирование по запросу пользователя Сканирование при обращении к файлам Сканирование по расписанию Сканирование сетевого трафика Ревизоры диска Встроенные антивирусы	*4*
	Практические занятия/ Лабораторные занятия: 1. Сканеры 2. Сканирование по запросу пользователя 3. Сканирование при обращении к файлам	*8*

	4. Сканирование по расписанию 5. Сканирование сетевого трафика 6. Ревизоры диска 7. Встроенные антивирус 8. Программа Kaspersky Anti-Virus 9. Программа Dr.Web 10.Программа Norton Antivirus 11.Прочие антивирусные программы 12.Программа Stop! 13.Программа Panda Antivirus 14.Программа Virus Scan	
	Консультации	
	Самостоятельная работа обучающихся: Доклад, разработка презентации к докладу на семинаре, поиск информации в сетях.	*2*
Тема 1.7. Антивирусы для интрасетей и для интернета	**Содержание учебного материала**	**8**
	Проблемы защиты крупных корпоративных интрасетей Функции удаленного управления и контроля Удаленное обновление антивирусных баз данных Децентрализованная установка и обновление антивирусов с сетевым центром управления Удаленная настройка антивирусных программ Обнаружение новых рабочих станций Планирование заданий Сигнальное информирование Архитектура и принципы работы корпоративных систем антивирусной защиты	*2*
	Практические занятия/ Лабораторные занятия: 1. Проблемы защиты крупных корпоративных интрасетей 2. Функции удаленного управления и контроля 3. Удаленное обновление антивирусных баз данных 4. Децентрализованная установка и обновление антивирусов с сетевым центром	*4*

	управления 5. Удаленная настройка антивирусных программ 6. Обнаружение новых рабочих станций 7. Планирование заданий 8. Сигнальное информирование 9. Архитектура и принципы работы корпоративных систем антивирусной защиты	
	Консультации	
	Самостоятельная работа обучающихся: Доклад, разработка презентации к докладу на семинаре, поиск информации в сетях.	*2*
Раздел 2. Методы защиты деструктивного воздействия		
Тема 2.1. Установка и удаление программы Dr.Web для Windows	**Содержание учебного материала**	**7**
	Состав дистрибутива Сканер Dr.Web Сторож SpIDer Guard Почтовый сторож SpIDer Mail Планировщик заданий Утилита обновления Процедура установки пакета Dr.Web для Windows Удаление пакета Dr.Web для Windows	*2*
	Практические занятия/ Лабораторные занятия: 1. Состав дистрибутива 2. Сканер Dr.Web 3. Сторож SpIDer Guard 4. Почтовый сторож SpIDer Mail 5. Планировщик заданий 6. Утилита обновления 7. Процедура установки пакета Dr.Web для Windows 8. Удаление пакета Dr.Web для Windows	*4*

	Консультации	
	Самостоятельная внеаудиторная работа:	*1*
Тема 2.2. Настройка пакета Dr.Web для Windows	**Содержание учебного материала**	**7**
	Стандартный пакет Dr.Web для Windows и пакет Dr.Web Home Edition Параметры проверки объектов Принципы отбора файлов для сканирования Настройка реакции программы на события Настройка ведения отчета Настройка звуковых реакций программы Настройка средств обновления Настройка системных установок	*2*
	Практические занятия/ Лабораторные занятия: 1. Стандартный пакет Dr.Web для Windows и пакет Dr.Web Home Edition 2. Параметры проверки объектов 3. Принципы отбора файлов для сканирования 4. Настройка реакции программы на события 5. Настройка ведения отчета 6. Настройка звуковых реакций программы 7. Настройка средств обновления 8. Настройка системных установок	*4*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме.	*1*
Тема 2.3. Защита почтовых систем	**Содержание учебного материала**	**5**
	Общие сведения. Возможные схемы защиты. Требования к антивирусному комплексу для проверки почтового потока. Параметры командной строки. Обнаружение вирусов Справочная система программы	*2*
	Практические занятия/ Лабораторные занятия: 1. Параметры командной строки	*2*

	2. Обнаружение вирусов 3. Справочная система программы	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме.	*1*
Тема 2.4. Почтовый антивирусный сторож SpIDer Mail	**Содержание учебного материала**	**5**
	Параметры командной строки Обнаружение вирусов Справочная система программы	*2*
	Практические занятия/ Лабораторные занятия: 1. Параметры командной строки 2. Обнаружение вирусов 3. Справочная система программы	*2*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме.	*1*
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	
Тема 2.5. Антивирусный комплекс ESET Nod32/Ср/	**Содержание учебного материала**	**7**
	Состав дистрибутива пакета ESET Nod32/Ср/ Установка и удаление пакета ESET Nod32/Ср/ Требования к установленным программам Требования к конфигурации компьютера Особенности пакета ESET Nod32/Ср/ Конфигурация пакета ESET Nod32/Ср/ Удаление пакета ESET Nod32/Ср/ Ознакомительная версия пакета Dr.Web для Unix Установка файла регистрационного ключа Обновление пакета ESET Nod32/Ср/ для Unix Вирусные базы данных пакета ESET Nod32/Ср/ для Unix	*2*

	Практические занятия/ Лабораторные занятия: 1. Состав дистрибутива пакета ESET Nod32/Ср/ 2. Установка и удаление пакета ESET Nod32/Ср/ 3. Требования к установленным программам 4. Требования к конфигурации компьютера 5. Особенности пакета ESET Nod32/Ср/ 6. Конфигурация пакета ESET Nod32/Ср/ 7. Удаление пакета ESET Nod32/Ср/ 8. Ознакомительная версия пакета Dr.Web для Unix 9. Установка файла регистрационного ключа 10.Обновление пакета ESET Nod32/Ср/ для Unix 11.Вирусные базы данных пакета ESET Nod32/Ср/ для Unix	*4*
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*1*
Тема 2.6. Мобильные антивирусы: защита планшетов и телефонов	**Содержание учебного материала**	**7**
	Запуск сканера Параметры командной строки Параметры проверки объектов Действия при обнаружении вирусов Принципы отбора файлов для сканирования Настройка реакции сканера на события Настройка ведения отчета	*2*
	Практические занятия/ Лабораторные занятия: 1. Запуск сканера 2. Параметры командной строки 3. Параметры проверки объектов 4. Действия при обнаружении вирусов 5. Принципы отбора файлов для сканирования 6. Настройка реакции сканера на события 7. Настройка ведения отчета	*4*

	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*1*
Тема 2.7. **Защита серверов и рабочих станций Kaspersky 6.0 для Windows**	**Содержание учебного материала**	***7***
	Состав дистрибутива Установка и настройка Требования к операционной системе Требования к установленным программам Требование к квалификации пользователя Процесс установки Конфигурация Kaspersky 6.0 для Windows Параметры проверки объектов Принципы отбора файлов для сканирования Настройка реакции программы на события Настройка ведения отчета Настройка реакций программы Настройка средств обновления Удаление Kaspersky 6.0 для Windows	*2*
	Практические занятия/ Лабораторные занятия: 1. Состав дистрибутива 2. Установка и настройка 3. Требования к операционной системе 4. Требования к установленным программам 5. Требование к квалификации пользователя 6. Процесс установки 7. Конфигурация Kaspersky 6.0 для Windows 8. Параметры проверки объектов 9. Принципы отбора файлов для сканирования 10. Настройка реакции программы на события 11. Настройка ведения отчета 12. Настройка реакций программы	*4*

	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*1*
Тема 2.8. Антивирусные решения компании Sophos	**Содержание учебного материала**	***7***
	Состав дистрибутива Установка пакета Sophos Small Business Suite Первый этап установки Второй этап установки Установка вручную Установка на компьютеры, не подключенные к Интернету Просмотр состояния антивирусной защиты на узлах сети Добавление новых компьютеров Обновление антивирусов и антивирусной базы данных Проверка файлов в автоматическом режиме Удаление вирусов Настройка извещений о вирусном заражении Настройка параметров антивирусной защиты рабочих станций Настройка параметров сканирования Настройка параметров удаления вирусов Настройка параметров антивирусной проверки Исключение файлов и дисков из проверки	*2*
	Практические занятия/ Лабораторные занятия: 1. Состав дистрибутива 2. Установка пакета Sophos Small Business Suite 3. Первый этап установки 4. Второй этап установки 5. Установка вручную 6. Установка на компьютеры, не подключенные к Интернету 7. Просмотр состояния антивирусной защиты на узлах сети 8. Добавление новых компьютеров 9. Обновление антивирусов и антивирусной базы данных	*4*

	10.Проверка файлов в автоматическом режиме 11.Удаление вирусов 12. Настройка извещений о вирусном заражении 13. Настройка параметров антивирусной защиты рабочих станций 14.Настройка параметров сканирования 15.Настройка параметров удаления вирусов 16.Настройка параметров антивирусной проверки 17.Исключение файлов и дисков из проверки	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*1*
Примерная тематика курсовой работы (проекта) *(если предусмотрены)*		*не предусмотрено*
Самостоятельная работа обучающихся над курсовой работой (проектом) *(если предусмотрены)*		*не предусмотрено*
	Всего:	***112***

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия мультимедийной аудитории (с установленным проектором) и компьютерного кабинета.

Оборудование лаборатории и рабочих мест лаборатории:

- автоматизированное рабочее место преподавателя;
- автоматизированное рабочие места обучающихся (по количеству обучающихся в подгруппе);
- сетевое периферийное оборудование;
- периферийное оборудование для ввода и вывода информации;
- мультимедийное оборудование: проектор, экран;
- комплект учебно-наглядных пособий «Антивирусные системы».
- файловый сервер, локальная сеть;
- выход в глобальную сеть;
- комплект учебно-методической документации

Программное обеспечение:

Android Studio, Brackets, Google Chrome, IIS Express, IntelliJ IDEA Community Edition,
Java SE Development Kit, Microsoft Visual Studio Code, PascalABC.Net, PostgreSQL 12,
Unity, Visual Studio Community 2019, WinRAR, XAMPP, Windows 10 Pro, Microsoft Office 2016, Visio 2016, Adobe Photoshop

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/476997
2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2021. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/470351

Дополнительная литература:

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495525
2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/475889
3. Сологубова, Г. С. Составляющие цифровой трансформации : монография / Г. С. Сологубова. — Москва : Издательство Юрайт, 2021. — 147 с. — (Актуальные монографии). — ISBN 978-5-534-11335-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/475065
4. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/467370

Интернет-ресурсы:

1. Библиотека Альдебаран – компьютерная литература [Электронный ресурс]. – Режим доступа: http://www.aldebarans.ru/komp, свободный. – Загл. с экрана.
2. Википедия – Свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org, свободный. – Загл. с экрана.
3. Официальный сайт Министерства образования и науки Российской Федерации. – Режим доступа: http://www.mon.gov.ru, свободный. – Загл. с экрана.
4. Педагогика.ру – Справочный сайт [Электронный ресурс]. – Режим доступа: http://www.pedagogy.ru, свободный. – Загл. с экрана.
5. Портал нормативно-технической документации [Электронный ресурс]. – Режим доступа: http://www.pntdoc.ru, свободный. – Загл. с экрана.
6. Российское образование. Федеральный портал [Электронный ресурс].. – Режим доступа: http://www.edu.ru, свободный. – Загл. с экрана.
7. Техническая литература [Электронный ресурс]. – Режим доступа: http://www.tehlit.ru, свободный. – Загл. с экрана

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
В результате освоения дисциплины обучающийся должен **уметь:** – организовывать антивирусную защиту информационной системы с помощью антивирусного программного обеспечения ; – осуществлять оперативное управление антивирусной безопасностью; – обнаруживать, анализировать и удалять компьютерные вирусы и другие вредоносные программы;	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; Экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
В результате освоения дисциплины обучающийся должен **знать:** - методы проникновения вирусов в систему; - способы маскировки и воспроизведения; - методы защиты от компьютерных вирусов; - принципы разработки и применения антивирусного программного обеспечения; - способы организации целостной системы антивирусной безопасности;	Интерпретация результатов устного опроса. Текущий контроль в форме тестирования. Текущий контроль усвоения материала в форме комбинированного опроса. Экспертная оценка результатов выполнения домашнего задания. Текущий контроль в форме комбинированного опроса. Экспертная оценка результатов выполнения домашнего задания.