Автономная некоммерческая организация среднего профессионального образования
«Колледж Волжского университета имени В.Н. Татищева»

УТВЕРЖДЕНО
приказом генерального директора
АНО СПО «Колледж ВУиТ»
И.А. Поленовой
от 22 мая 2023 г. №82

Рабочая программа дисциплины

ОП.19 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

профессионального цикла

основной профессиональной образовательной программы по специальности

09.02.01 Компьютерные системы и комплексы

Тольятти, 2023 г.

ОДОБРЕНА
Педагогическим Советом
Протокол № 5 от «22» мая 2023г.

Составитель: Мигунова Елена Григорьевна, заведующая отделением «Сервиса и информационных технологий» АНО СПО «Колледж ВУиТ».

Рабочая программа разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности **09.02.01 Компьютерные системы и комплексы**, утвержденной приказом Министерства образования и науки РФ от «28» июля 2014 г. № 849

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.19 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Область применения программы

Рабочая программа учебной дисциплины (далее программа УД) - является частью основной профессиональной образовательной программы АНО СПО «Колледж ВУиТ» по специальности СПО 09.02.01 Компьютерные системы и комплексы.

Рабочая программа составлена для очной формы обучения.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы: рабочая программа входит в обязательную часть профессионального цикла.

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

Базовая часть

В результате освоения дисциплины студент должен **уметь:**

- обоснованно выбирать необходимые для выполнения задач информационной безопасности политику и модели безопасности компьютерных систем и комплексов;
- использовать технологии защиты информации при решении задач управления компьютерных систем и комплексов.

В результате освоения дисциплины студент должен **знать:**

- основы организации отечественных и международных стандартов в области информационной безопасности;
- методы соблюдения требований информационной безопасности.

Вариативная часть – не предусмотрено.

Содержание дисциплины должно быть ориентировано на подготовку студентов к освоению профессиональных модулей ОПОП по специальности 09.02.01 Компьютерные системы и комплексы и овладению **профессиональными компетенциями** (ПК):

ПК 1.5. Выполнять требования нормативно-технической документации.

В процессе освоения дисциплины у студентов должны формироваться **общие компетенции (ОК):**

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 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

1.4. Количество часов на освоение программы учебной дисциплины:

Максимальная учебная нагрузка 120 часов, в том числе:

Обязательная аудиторная учебная нагрузка – 85 часов;

Самостоятельная работа – 35 часов.

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объём учебной дисциплины и виды учебной работы

Вид учебной деятельности	Объем часов
Максимальная учебная нагрузка (всего)	120
Обязательная аудиторная учебная нагрузка (всего)	85
в том числе:	
лабораторные занятия	-
практические занятия	17
контрольные работы	-
курсовая работа (проект)	-
самостоятельная работа студента (всего)	35
Итоговая аттестация	Зачет

2.2. Тематический план и содержание учебной дисциплины ОП.19 Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
Раздел 1. Информационная безопасность и уровни ее обеспечения			
Тема 1.1. Понятие "информационная безопасность"	**Содержание учебного материала** Различные подходы к определению понятия "информационная безопасность", задачи информационной безопасности, уровни формирования режима информационной безопасности	2	1
Тема 1.2. Составляющие информационной безопасности	**Содержание учебного материала** Составляющие понятия "информационная безопасность", определение целостности информации, определения конфиденциальности и доступности информации.	2	1
Тема 1.3. Система формирования режима информационной безопасности	**Содержание учебного материала** Задачи информационной безопасности, уровни формирования режима информационной безопасности, особенности законодательно-правового и административного уровней, подуровни программно-технического уровня.	2	1
	Практическое занятие №1 Распределение задач информационной безопасности по уровням ее обеспечения	1	2
Тема 1.4. Нормативно-правовые основы информационной безопасности в РФ	**Содержание учебного материала** нормативно-правовые основы информационной безопасности общества; основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации, ответственность за нарушения в сфере информационной безопасности.	2	1
Тема 1.5. Стандарты информационной безопасности: "Общие критерии	**Содержание учебного материала** Основное содержание оценочного стандарта ISO/IEC 15408, отличия функциональных требований от требований доверия, классы функциональных требований и требований доверия.	2	1
Тема 1.6. Стандарты информационной безопасности распределенных систем	**Содержание учебного материала** основное содержание стандартов по информационной безопасности распределенных систем, основные сервисы безопасности в вычислительных сетях, наиболее эффективные механизмы безопасности, задачи администрирования средств безопасности.	4	1

Тема 1.7. Стандарты информационной безопасности в РФ	**Содержание учебного материала** Роли Гостехкомиссии в обеспечении информационной безопасности в РФ, документы по оценке защищенности автоматизированных систем в РФ.	2	1
Тема 1.8. Административный уровень обеспечения информационной безопасности	**Содержание учебного материала** цели и задачи административного уровня обеспечения информационной безопасности, содержание административного уровня, направления разработки политики безопасности	2	1
Тема 1.9. Информационная безопасность в РФ	**Содержание учебного материала** Определение политики безопасности организации, Конституция Российской Федерации, доктрина информационной безопасности Российской Федерации, федеральные законы в области информации и информационной безопасности, указы президента РФ и постановления правительства РФ в области информации и информационной безопасности, правовые режимы защиты информации.	2	1
Тема 1.10. Классификация угроз "информационной безопасности"	**Содержание учебного материала** классы угроз информационной безопасности, причины и источники случайных воздействий на информационные системы, каналы несанкционированного доступа к информации	4	1
	Практическое занятие №2 Методы выявления и классифицировать угрозы информационной безопасности.	1	2
Самостоятельная работа	Подготовка доклада с презентацией по темам раздела	5	3
Раздел 2. Компьютерные вирусы и защита от них.			
Тема 2.1. Вирусы как угроза информационной безопасности	**Содержание учебного материала** Характерные черты компьютерных вирусов, проблемы при определении компьютерного вируса.	2	1
Тема 2.2. Классификация компьютерных вирусов	**Содержание учебного материала** Классы компьютерных вирусов, характеристику различных компьютерных вирусов	2	1
Тема 2.3. Характеристика "вирусоподобных" программ	**Содержание учебного материала** Виды "вирусоподобных" программ, деструктивные возможности "вирусоподобных" программ.	2	1
Тема 2.4.	**Содержание учебного материала**	2	1

Антивирусные программы	Виды антивирусных программ, принципы функционирования антивирусных программ, факторы, определяющие качество антивирусной программы. Студент должен уметь, классифицировать антивирусные программы.		
Тема 2.5. Профилактика компьютерных вирусов	**Содержание учебного материала** Наиболее распространенные пути заражения компьютеров вирусами, правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей	4	1
	Практическое занятие № 3 Методы профилактики компьютерных вирусов.	2	2
Тема 2.6. Обнаружение неизвестного вируса	**Содержание учебного материала** Общий алгоритм обнаружения неизвестного вируса.	4	1
	Практическое занятие № 4 Проверка систему на наличие макровируса	2	2
Самостоятельная работа	Подготовка доклада с презентацией по темам раздела	10	3
Раздел 3. Информационная безопасность вычислительных сетей			
Тема 3.1. Особенности обеспечения информационной безопасности в компьютерных сетях	**Содержание учебного материала** Особенности обеспечения информационной безопасности компьютерных сетей, основные цели информационной безопасности компьютерных сетей, специфику методов и средств защиты компьютерных сетей.	2	1
Тема 3.2. Сетевые модели передачи данных	**Содержание учебного материала** Теоретические основы построения компьютерных сетей, протоколы передачи данных.	2	1
Тема 3.3. Модель взаимодействия открытых систем OSI/ISO	**Содержание учебного материала** Структура модели открытых систем OSI/ISO и назначение ее уровней	2	1
	Практическое занятие № 5 Использование модель OSI/ISO для описания процесса передачи данных между узлами компьютерной сети.	2	2
Тема 3.4. Адресация в глобальных сетях	**Содержание учебного материала** Принципы адресации в современных вычислительных сетях, классы адресов протокола IP и структуру IP-адреса, иерархический принцип системы доменных имен	2	1
	Практическое занятие № 6 Преобразование двоичного IP-адреса в десятичный, определение типа сети по IP-адресу.	2	2

Тема 3.5. Классификация удаленных угроз в вычислительных сетях	**Содержание учебного материала** Классы удаленных угроз и их характеристики.	2	1
Тема 3.6. Типовые удаленные атаки и их характеристика	**Содержание учебного материала** Типовые удаленные атаки и механизмы их реализации.	2	1
	Практическое занятие № 7 Классификация типовых удаленных атак по совокупности признаков.	2	2
Тема 3.7. Причины успешной реализации удаленных угроз в вычислительных сетях	**Содержание учебного материала** Причины успешной реализации удаленных угроз информационной безопасности в вычислительных сетях, реализация принципов.	2	1
Тема 3.8. Принципы защиты распределенных вычислительных сетей	**Содержание учебного материала** Принципы защиты распределенных вычислительных сетей.	2	1
Самостоятельная работа	Подготовка доклада с презентацией по темам раздела	10	3
Раздел 4. Механизмы обеспечения "информационной безопасности"			
Тема 4.1. Идентификация и аутентификация	**Содержание учебного материал** Механизмы идентификации и аутентификации, идентификаторы, используемые при реализации механизма идентификации и аутентификации.	2	1
	Практическое занятие № 8 Механизмы идентификации и аутентификации.	1	2
Тема 4.2. Криптография и шифрование	**Содержание учебного материала** структуру криптосистемы, методы шифрования данных.	2	1
	Практическое занятие № 9 Использование электронную цифровую подпись для проверки целостности данных.	2	2
Тема 4.3. Методы разграничение доступа	**Содержание учебного материала** Методы разграничения доступа, методы управления доступом, предусмотренные в руководящих документах Гостехкомиссии.	2	1
	Практическое занятие № 10 Методы разграничения доступа.	2	2
Тема 4.4.	**Содержание учебного материала**	2	1

Регистрация и аудит	Защитные свойства механизма регистрации и аудита, методы аудита безопасности информационных систем. Использовать механизмы регистрации и аудита для анализа защищенности системы.		
Тема 4.5. Межсетевое экранирование	**Содержание учебного материала** Механизм межсетевого экранирования.	2	2
Тема 4.6. Технология виртуальных частных сетей (VPN)	**Содержание учебного материала** Составляющие технологии виртуальных частных сетей.	2	1
Самостоятельная работа	Подготовка доклада с презентацией по темам раздела	10	3
Зачет			
	Всего:	**120**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1 – ознакомительный (узнавание ранее изученных объектов, свойств)
2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия Лаборатории информационных технологий.

Оборудование учебного кабинета:

- 9 двухместных ученических столов;
- стулья на 28 посадочных мест;
- учебная доска;
- 8 персональных компьютеров;
- коммутатор 24 портовый;
- сетевой фильтр.

Рабочее место преподавателя:

- стол;
- стул.

3.2. Информационное обеспечение

Информационное обеспечение обучения содержит перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы.

Основные источники:

1. Партыка, Т.Л. Информационная безопасность: учеб. пособие для СПО рек. МО. - М.: ФОРУМ: ИНФРА-М, 2007. - 365 с.

2. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189328.

Дополнительные источники:

1. Башлы, П. Н. Информационная безопасность: учеб. пособие для СПО рек. МО. - Ростов н/Д: Феникс, 2006. - 254 с.

2. Мельников, В. П. Информационная безопасность: учеб. пособие для СПО. - М: Академия, 2005. - 336 с.

Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2023. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1910870.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
В результате освоения дисциплины студент **должен уметь:**	
- обоснованно выбирать необходимые для выполнения задач информационной безопасности политику и модели безопасности компьютерных систем и комплексов; - использовать технологии защиты информации при решении задач управления компьютерных систем и комплексов.	Проверка и оценка выполнения студентом самостоятельной работы. Оценивание качества выполнения практических работ. Опросы и беседы по материалу домашних заданий и лекций. Экспертная оценка во время сдачи зачета.
В результате освоения дисциплины студент **должен знать:**	
- основы организации отечественных и международных стандартов в области информационной безопасности; - методы соблюдения требований информационной безопасности.	Проверка и оценка выполнения студентом самостоятельной работы. Оценивание качества выполнения практических работ. Опросы и беседы по материалу домашних заданий и лекций. Экспертная оценка во время сдачи зачета.