

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Поленова Инна Александровна

Должность: Генеральный директор

Дата подписания: 18.10.2023 13:04:24

Уникальный программный ключ:

2bc51b031f52f1ef87c6946d50ac9f5ab912348ab42251f7e55eb40acef68095

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 УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.16 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Общепрофессионального цикла

основной профессиональной образовательной программы по специальности

09.02.01 Компьютерные системы и комплексы

квалификация выпускника – специалист по компьютерным системам

Тольятти, 2023 год

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**, утвержденного Приказом Минпросвещения России от 25 мая 2022г. № 362

СОДЕРЖАНИЕ

1	ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	4
2	СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	5
3	УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ	11
4	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	12

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.16 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:

Учебная дисциплина «Информационная безопасность» входит в вариативную часть общепрофессионального цикла.

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

Вариативная 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.

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)**:

Код	Наименование результата обучения
ПК 1.1.	Анализировать требования технического задания на проектирование цифровых систем

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

ОК 1	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 2	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК 9	Пользоваться профессиональной документацией на государственном и иностранном языках

1.4. Количество часов на освоение программы учебной дисциплины:

- максимальная учебная нагрузка **85 часов**, в том числе;
- обязательная аудиторная учебная нагрузка – **80 часов**;
- самостоятельная работа – **5 часов**.

В том числе часов **вариативной части** учебных циклов ППССЗ: **85 часов**

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной деятельности	Объем часов
Максимальная учебная нагрузка (всего)	85
Обязательная аудиторная учебная нагрузка (всего)	80
в том числе:	
лабораторные занятия	-
практические занятия	16
контрольные работы	-
курсовая работа (проект)	-
самостоятельная работа студента (всего)	5
Промежуточная аттестация в форме	<i>Зачета с оценкой</i>

2.2. Тематический план и содержание учебной дисциплины ОП.16 Информационная безопасность

Наименование разделов и тем 1	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся 2	Объем часов 3	Уровень освоения 4
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 2	 1
Тема 1.2. Составляющие информационной безопасности	Содержание учебного материала Составляющие понятия "информационная безопасность", определение целостности информации, определения конфиденциальности и доступности информации.	2 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 2	 1
	Практическое занятие №1 Распределение задач информационной безопасности по уровням ее обеспечения	1	2,3
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 2	 1
Тема 1.5. Стандарты информационной безопасности: "Общие критерии"	Содержание учебного материала	2	

	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	4	
	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	2	
	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	2	
	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	2	
	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	5/1	
	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	1	3
Раздел 2. Компьютерные вирусы и защита от них.			
Тема 2.1.	Содержание учебного материала	2	

Вирусы как угроза информационной безопасности	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	
		2	1
Тема 2.3. Характеристика "вирусоподобных" программ	Содержание учебного материала Виды "вирусоподобных" программ, деструктивные возможности "вирусоподобных" программ.	2	1
Тема 2.4. Антивирусные программы	Содержание учебного материала Виды антивирусных программ, принципы функционирования антивирусных программ, факторы, определяющие качество антивирусной программы. Студент должен уметь, классифицировать антивирусные программы.	2	1
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	4/2	
	Практическое занятие № 3 Методы профилактики компьютерных вирусов.	2	2,3
Тема 2.6. Обнаружение неизвестного вируса	Содержание учебного материала Общий алгоритм обнаружения неизвестного вируса.	4/2	
	Практическое занятие № 4 Проверка систему на наличие макровируса	2	1
	Самостоятельная работа Подготовка доклада с презентацией по темам раздела	2	2
		2	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	
		2	1
Тема 3.2. Сетевые модели передачи данных	Содержание учебного материала Теоретические основы построения компьютерных сетей, протоколы передачи данных.	2	
		2	1

Тема 3.3. Модель взаимодействия открытых систем OSI/ISO	Содержание учебного материала	4/2	
	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	2,3
Тема 3.4. Адресация в глобальных сетях	Содержание учебного материала	4/2	
	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	2,3
Тема 3.5. Классификация удаленных угроз в вычислительных сетях	Содержание учебного материала	2	
	Классы удаленных угроз и их характеристики.	2	1
Тема 3.6. Типовые удаленные атаки и их характеристика	Содержание учебного материала	3/1	
	Типовые удаленные атаки и механизмы их реализации.	2	1
	Практическое занятие № 7 Классификация типовых удаленных атак по совокупности признаков.	1	2,3
Тема 3.7. Причины успешной реализации удаленных угроз в вычислительных сетях	Содержание учебного материала	2	
	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	3/1	
	Принципы защиты распределенных вычислительных сетей.	2	1
	Самостоятельная работа		
	Подготовка доклада с презентацией по темам раздела	1	3
Раздел 4. Механизмы обеспечения "информационной безопасности"			
Тема 4.1. Идентификация и аутентификация	Содержание учебного материал	3/1	
	Механизмы идентификации и аутентификации, идентификаторы, используемые при реализации механизма идентификации и аутентификации.	2	1
	Практическое занятие № 8 Механизмы идентификации и аутентификации.	1	2,3

Тема 4.2. Криптография и шифрование	Содержание учебного материала	4/2	
	Структура 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	4/2	
	Методы разграничения доступа, методы управления доступом, предусмотренные в руководящих документах Гостехкомиссии.	2	1
	Практическое занятие № 10 Методы разграничения доступа.	2	2,3
Тема 4.4. Регистрация и аудит	Содержание учебного материала	2	
	Защитные свойства механизма регистрации и аудита, методы аудита безопасности информационных систем. Использовать механизмы регистрации и аудита для анализа защищенности системы.	2	1
Тема 4.5. Межсетевое экранирование	Содержание учебного материала	2	
	Механизм меж сетевого экранирования.	2	1
Тема 4.6. Технология виртуальных частных сетей (VPN)	Содержание учебного материала	2	
	Составляющие технологии виртуальных частных сетей.	2	1
	Самостоятельная работа Подготовка доклада с презентацией по темам раздела	1	3
7 семестр	Промежуточная аттестация в форме зачета с оценкой	Л-64 Пр-16 Ср-5	
Всего:		85	

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»:

Перечень основного оборудования, учебно-наглядных пособий и используемого программного обеспечения:

офисная мебель на 16 мест, 8 ПК с доступом в Интернет и ЭИОС.

WindowsXP, OpenOffice, 7-zip, Microsoft Word Viewer, Microsoft Exel Viewer, Microsoft PowerPoint Viewer, СПС КонсультантПлюс, 1С: Бухгалтерия 8

3.2. Информационное обеспечение

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

Основные источники:

1. 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>.

2. 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>.

3. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1898839>.

4.

Дополнительные источники:

1. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1862651>.

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

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

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:	
<ul style="list-style-type: none"> - 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. 	<p>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.</p>
В результате освоения дисциплины студент должен знать:	
<ul style="list-style-type: none"> - основы организации отечественных и международных стандартов в области информационной безопасности; - методы соблюдения требований информационной безопасности. 	<p>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.</p>