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

УТВЕРЖДАЮ
Генеральный директор
АНО СПО «Колледж ВУиТ»
_____ И.А. Поленова
29 августа 2018 г.

Рабочая программа дисциплины

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

по специальности

09.02.01 Компьютерные системы и комплексы

квалификация выпускника – техник по компьютерным системам

Тольятти

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии по специальности 09.02.01 Компьютерные системы и комплексы.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы: входит в профессиональный цикл общепрофессиональных дисциплин ОП.18.

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

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

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

В процессе изучения дисциплины у обучающихся формируются компетенции, включающие в себя способность:

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.
ПК 1.5.	Выполнять требования нормативно-технической документации.

1.4. Рекомендуемое количество часов на освоение программы 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 работы	Количество часов
Максимальная учебная нагрузка (всего)	**120**
Обязательная аудиторная нагрузка (всего)	**85**
в том числе:	
практические занятия	**17**
Самостоятельная работа обучающегося (всего)	**35**
Итоговая аттестация в форме зачета	

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов
Раздел 1. Информационная безопасность и уровни ее обеспечения		**31**
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
Тема 1.2. Составляющие информационной безопасности	**Содержание учебного материала** Составляющие понятия "информационная безопасность", определение целостности информации, определения конфиденциальности и доступности информации.	2
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
	Практическое занятие №1 Распределение задач информационной безопасности по уровням ее обеспечения	1
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
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
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

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов
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
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
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
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
	Практическое занятие №2 Методы выявления и классифицировать угрозы информационной безопасности.	1
Самостоятельная работа	Подготовка доклада с презентацией по темам раздела	5
Раздел 2. Компьютерные вирусы и защита от них.		**30**
Тема 2.1. Вирусы как угроза информационной безопасности	**Содержание учебного материала** Характерные черты компьютерных вирусов, проблемы при определении компьютерного вируса.	2
Тема 2.2. Классификация компьютерных вирусов	**Содержание учебного материала** Классы компьютерных вирусов, характеристику различных компьютерных вирусов	2
Тема 2.3. Характеристика	**Содержание учебного материала** Виды "вирусоподобных" программ, деструктивные возможности "вирусоподобных"	2

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов
"вирусоподобных" программ	программ.	
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
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
	Практическое занятие № 3 Методы профилактики компьютерных вирусов.	2
Тема 2.6. Обнаружение неизвестного вируса	**Содержание учебного материала** Общий алгоритм обнаружения неизвестного вируса.	4
	Практическое занятие № 4 Проверка систему на наличие макровируса	2
Самостоятельная работа	Подготовка доклада с презентацией по темам раздела	10
Раздел 3. Информационная безопасность вычислительных сетей		**32**
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
Тема 3.2. Сетевые модели передачи данных	**Содержание учебного материала** Теоретические основы построения компьютерных сетей, протоколы передачи данных.	2
Тема 3.3. Модель взаимодействия открытых систем OSI/ISO	**Содержание учебного материала** Структура модели открытых систем OSI/ISO и назначение ее уровней	2
	Практическое занятие № 5 Использование модель OSI/ISO для описания процесса передачи данных между узлами компьютерной сети.	2

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов
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
	Практическое занятие № 6 Преобразование двоичного IP-адреса в десятичный, определение типа сети по IP-адресу.	2
Тема 3.5. Классификация удаленных угроз в вычислительных сетях	**Содержание учебного материала** Классы удаленных угроз и их характеристики.	2
Тема 3.6. Типовые удаленные атаки и их характеристика	**Содержание учебного материала** Типовые удаленные атаки и механизмы их реализации.	2
	Практическое занятие № 7 Классификация типовых удаленных атак по совокупности признаков.	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
Тема 3.8. Принципы защиты распределенных вычислительных сетей	**Содержание учебного материала** Принципы защиты распределенных вычислительных сетей.	2
Самостоятельная работа	Подготовка доклада с презентацией по темам раздела	10
Раздел 4. Механизмы обеспечения "информационной безопасности"		**27**
Тема 4.1. Идентификация и аутентификация	**Содержание учебного материал** Механизмы идентификации и аутентификации, идентификаторы, используемые при реализации механизма идентификации и аутентификации.	2
	Практическое занятие № 8 Механизмы идентификации и аутентификации.	1
Тема 4.2. Криптография и шифрование	**Содержание учебного материала** структуру криптосистемы, методы шифрования данных.	2

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов
	Практическое занятие № 9 Использование электронную цифровую подпись для проверки целостности данных.	2
Тема 4.3. Методы разграничение доступа	**Содержание учебного материала** Методы разграничения доступа, методы управления доступом, предусмотренные в руководящих документах Гостехкомиссии.	2
	Практическое занятие № 10 Методы разграничения доступа.	2
Тема 4.4. Регистрация и аудит	**Содержание учебного материала** Защитные свойства механизма регистрации и аудита, методы аудита безопасности информационных систем. Использовать механизмы регистрации и аудита для анализа защищенности системы.	2
Тема 4.5. Межсетевое экранирование	**Содержание учебного материала** Механизм межсетевого экранирования.	2
Тема 4.6. Технология виртуальных частных сетей (VPN)	**Содержание учебного материала** Составляющие технологии виртуальных частных сетей.	2
Самостоятельная работа	Подготовка доклада с презентацией по темам раздела	10
	Итого	**120**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Лаборатория информационных технологий.

Рабочее место преподавателя: стол, стул;9 двухместные ученические столы и стулья на 28 посадочных мест, учебная доска, 8 персональных компьютеров, коммутатор 24 портовый, сетевой фильтр.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

3.2.1 Основные источники:

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

2. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для СПО/ Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; отв. ред. Т. А. Полякова, А. А. Стрельцов. — М.: Издательство Юрайт, 2018. — 325 с.//режим доступа «ЭБС Юрайт».

3. Нестеров, С. А. Информационная безопасность: учебник и практикум для академического бакалавриата / С. А. Нестеров. — М.: Издательство Юрайт, 2018. — 321 с.//режим доступа «ЭБС Юрайт».

3.2.2 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.

3.2.3 При проведении занятий по дисциплине используются следующие программные продукты:

1. ОС Windows (для академических организаций, лицензия Microsoft Imagine (ранее MSDN AA, DreamSpark);
2. Интернет-браузеры: Google Chrome (свободное ПО), Internet Explorer 8 (свободное ПО);
3. Microsoft Word 2007 (правом пользования обладает stud, номер продукта: 89396-711-8663723-65209).
4. Справочно-поисковые системы (КонсультантПлюс и/или Гарант);
5. Доступ к электронным изданиям ЭБС ЮРАЙТ (www.biblio-online.ru).

4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

При освоении программы у обучающихся формируются компетенции – знания, умения и навыки по данному предмету, необходимые для изучения других предметов, и для использования в ходе изучения специальных дисциплин профессионального цикла, в практической деятельности и повседневной жизни.

Результаты обучения (освоенные умения, усвоенные)	**Формы и методы контроля и оценки результатов обучения**
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.	Оценка результатов: - аудиторных практических работ; - внеаудиторной самостоятельной работы: доклады.
Знать: основы организации отечественных и международных стандартов в области информационной безопасности; методы соблюдения требований информационной безопасности.	Оценка результатов: - аудиторных практических работ; - внеаудиторной самостоятельной работы: доклады.