МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
имени В.Я. Горина»

Факультет среднего профессионального образования

«Утверждаю»
Декан факультета среднего
профессионального образования
___________ Бражник Г.В.
«_04_» _июля_ 2019 года

Факультет среднего проф. образования

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

специальность 09.02.05 – Прикладная информатика (по отраслям)
(базовый уровень)

Майский, 2019

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (ФГОС СПО) по специальности 09.02.05 – Прикладная информатика (по отраслям), утвержденного приказом Министерства образовавния и науки Российской федерации 1001 от 13 августа 2014 года, на овновании «Разъяснений по формированию примерных программ учебных дисциплин начального профессионального образования на основе Федеральных государственных образовательных стандартов начального профессионального и среднего профессионального образования», утвержденных Департаментом государственной политики в образовании Министерства образования и науки Российской Федерации 27 августа 2009 г.

Организация-разработчик: ФГБОУ ВО Белгородский ГАУ

Разработчик(и): Михайлова В.Л., преподаватель кафедры информатики и и нформационноых технологий

Рассмотрена на заседании кафедры информатики и информационных технологий от
20.06 2019 г., протокол № 12

зав. кафедрой _____ Петросов Д.А.

Одобрена методической комиссией инженернорного факультета от 04.07. 2019 г., протокол № 7-В/19

Председатель методической комисии _____А.П. Слободюк

СОДЕРЖАНИЕ

	стр.
1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	4
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	6
3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	7
4. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ	11
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	13

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Область применения программы

Рабочая программа учебной дисциплины **«Информационная безопасность»** является частью ППССЗ в соответствии с ФГОС по специальности СПО 09.02.05 «Прикладная информатика», введена в учебный план в соответствии с ФГОС СПО за счет часов вариативной части.

Рабочая программа учебной дисциплины может быть использована для профессиональной подготовки техников-программистов.

1.2. Место учебной дисциплины в структуре ППССЗ:

Дисциплина «Информационная безопасность» входит в состав цикла общепрофессиональных дисциплин ОП.13.

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

В результате освоения учебной дисциплины обучающийся должен

Уметь:

-применять программное обеспечение для защиты от несанкционированного доступа;

-применять программное обеспечение для защиты от вирусного заражения компьютера;

-зашифровывать и дешифровывать сообщения различными методами;

-создавать открытый ключ и вырабатывать индивидуальный секретный ключ для документов с помощью программного обеспечения.

В результате освоения учебной дисциплины обучающийся должен

Знать:

- принципы системного подхода к защите информации;
- основные понятия криптографии,
- принципы передачи информации по каналам передачи;
- методы шифрования и дешифрования.

Результатом освоения учебной дисциплины **«Информационная безопасность»** является овладение профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК - 1.1	Обрабатывать статический информационный контент
ПК - 1.2	Обрабатывать динамический информационный контент
ПК - 1.5	Контролировать работу компьютерных, периферийных устройств и телекоммуникационных систем, обеспечивать их правильную эксплуатацию.
ПК - 3.3	Проводить обслуживание, тестовые проверки, настройку программного обеспечения отраслевой направленности.
ОК-1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК-2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество
ОК-3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК-4	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК-5	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК-6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями
ОК-7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК-8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК- 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

1.4. Количество часов на освоение рабочей программы учебной дисциплины:

максимальной учебной нагрузки обучающегося 84 часа, в том числе:

обязательной аудиторной учебной нагрузки 56 часов;

(28- часов лекций; 28- часов практических занятий);

самостоятельной работы - 28 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	84
Обязательная аудиторная учебная нагрузка (всего)	56
лекции	28
лабораторные работы	-
практические занятия	28
контрольные работы	-
курсовая работа (проект)	-
Самостоятельная работа обучающегося (всего)	28
Итоговая аттестация в форме зачёта	

2.2. Тематический план и содержание учебной дисциплины Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
РАЗДЕЛ 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И УРОВНИ ЕЕ ОБЕСПЕЧЕНИЯ		**24**	
Тема 1.1. Понятие «информационная безопасность». Составляющие информационной безопасности.	**Лекционное занятие.** Проблема информационной безопасности общества. Определение понятия «информационная безопасность». Составляющие информационной безопасности: доступность, целостность, конфиденциальность информации.	2	2
	Практическое занятие. Информация как объект защиты.	2	
	Самостоятельная работа. Подготовка реферата: Уровни обеспечения информационной безопасности.	2	
Тема 1.2. Система формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности РФ.	**Лекционное занятие.** Задачи информационной безопасности общества. Уровни формирования режима информационной безопасности. Правовые основы информационной безопасности общества. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации.	2	2
	Практическое занятие. Обеспечение информационной безопасности в ведущих зарубежных странах.	2	
	Самостоятельная работа. Подготовка реферата: Ответственность за нарушения в	2	

	сфере информационной безопасности.		
Тема 1.3. Стандарты информационной безопасности.	**Лекционное занятие.** Требования безопасности к информационным системам. Принцип иерархии. Стандарты информационной безопасности распределенных систем.	2	2
	Практическое занятие. Построение концепции информационной безопасности предприятия.	2	
	Самостоятельная работа. Подготовка реферата: Стандарты информационной безопасности в РФ.	2	
Тема 1.4. Административный уровень обеспечения информационной безопасности.	**Лекционное занятие.** Цели, задачи и содержание административного уровня. Разработка политики информационной безопасности.	2	2
	Практическое занятие. Анализ рисков информационной безопасности. Тестирование.	2	
	Самостоятельная работа. Подготовка реферата: Классификация угроз информационной безопасности.	2	
РАЗДЕЛ 2. КОМПЬЮТЕРНЫЕ ВИРУСЫ И ЗАЩИТА ОТ НИХ.		**18**	
Тема 2.1. Вирусы как угроза информационной безопасности. Профилактика компьютерных вирусов.	**Лекционное занятие.** Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов. Правила защиты от компьютерных вирусов.	2	2
	Практическое занятие. Пакеты вирусных программ.	2	
	Самостоятельная работа. Характеристика путей проникновения вирусов в компьютеры.	2	
Тема 2.2.	**Лекционное занятие.** Виды	2	2

Характеристика «вирусоподобных» программ.	«вирусоподобных программ» и их характеристика. Утилиты скрытого администрирования.		
	Практическое занятие. Способы обнаружения «вирусоподобных» программ. Решение кейс-задачи.	2	
	Самостоятельная работа. **Подготовка реферата:** Методы борьбы с распространением «вирусоподобных» программ.	2	
Тема 2.3. Антивирусные программы. Обнаружение неизвестного вируса.	**Лекционное занятие.** Особенности антивирусных программ. Классификация антивирусных программ. Обнаружение загрузочного вируса. Обнаружение резидентного вируса. Обнаружение макровируса.	2	2
	Практическое занятие. Работа с антивирусными программами. Тестирование.	2	
	Самостоятельная работа. **Подготовка реферата:** Факторы, определяющие качество антивирусных программ. Общий алгоритм обнаружения вируса.	2	
РАЗДЕЛ 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ.		**18**	
Тема 3.1. Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных.	**Лекционное занятие.** Особенности информационной безопасности в компьютерных сетях. Специфика средств защиты в компьютерных сетях. Принципы обмена данными в вычислительных сетях. Транспортный протокол TCP и модель TCP/IP.	2	2
	Практическое занятие. Обеспечение информационной безопасности в компьютерных сетях.	2	
	Самостоятельная работа.	2	

	Подготовка реферата: Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях.		
Тема 3.2. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика.	**Лекционное занятие.** Классы удаленных угроз и их характеристика. Типовые удаленные атаки и их характеристика.	2	2
	Практическое занятие. Анализ защищенности объекта защиты информации.	2	
	Самостоятельная работа. Подготовка реферата: Профилактика удаленных угроз в вычислительных сетях.	2	
Тема 3.3. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей.	**Лекционное занятие.** Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей.	2	2
	Практическое занятие. Построение модели потенциального нарушителя ИС. Тестирование.	2	
	Самостоятельная работа. Подготовка реферата: Защита от удаленных угроз в вычислительных сетях.	2	
РАЗДЕЛ 4. МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ «ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».		**24**	
Тема 4.1. Идентификация и аутентификация.	**Лекционное занятие.** Определение понятий «идентификация» и «аутентификация». Механизм идентификации и аутентификации пользователей.	2	2
	Практическое занятие. Парольная защита.	2	
	Самостоятельная работа. Подготовка реферата: Идентификация пользователя по голосу.	2	

Тема 4.2. Криптография и шифрование.	**Лекционное занятие.** Структура криптосистемы. Классификация систем шифрования данных. Симметричные и асимметричные методы шифрования. Механизм электронной цифровой подписи.	2	2
	Практическое занятие. Симметричные алгоритмы шифрования. Асимметричные алгоритмы шифрования. Решение кейс-задачи.	2	
	Самостоятельная работа. Подготовка реферата: Шифрование сообщений.	2	
Тема 4.3. Методы разграничения доступа	**Лекционное занятие.** Методы разграничения доступа. Мандатное и дискретное управление доступом.	2	2
	Практическое занятие. Механизмы контроля целостности данных.	2	
	Самостоятельная работа. Подготовка реферата: Средства контроля за разграничением прав доступа.	2	
Тема 4.4. Регистрация и аудит. Межсетевое экранирование.	**Лекционное занятие.** Регистрация и аудит. Межсетевое экранирование.	2	2
	Практическое занятие. Построение системы межсетевого экранирования.	2	
	Самостоятельная работа. Подготовка реферата: Технология виртуальных частных сетей (VPN).	2	
ИТОГО		**84**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия компьютерного класса

Кабинет архитектуры электронно-вычислительных машин и вычислительных систем № 312, 302, ул. Студенческая, 1. Лекционный компьютерный класс (302), компьютеры в сборе (Системный блок: ASRock H61M-DGS/ DualCore Intel Pentium G860, 3000 MHz / 8 Гб(4+4DDR3)/ ST250DM0/Intel HD Graphics; Монитор: Philips 233v5, клавиатура, мышь), столы, стулья, стенды, доска, видеокамера купольная
Лекционный компьютерный класс (312), компьютеры в сборе (Системный блок: ASRock H61M-DGS/ DualCore Intel Pentium G860, 3000 MHz/8Гб(4+4GbDDR3)/ ST250DM0 (250 Гб, 7200 RPM, SATA-III)/ ATAPI iHAS122; Монитор: Philips 233v5, клавиатура, мышь), столы, стулья, стенды, доска, видеокамера купольная
Помещение для самостоятельной работы
(библиотека, читальный зал с выходом в Интернет), ул. Вавилова, 24. Специализированная мебель; комплект компьютерной техники в сборе (системный блок: Asus P4BGL-MX\Intel Celeron, 1715 MHz\256 Мб PC2700 DDR SDRAM\ST320014A (20 Гб, 5400 RPM, Ultra-ATA/100)\ NEC CD-ROM CD-3002A\Intel(R) 82845G/GL/GE/PE/GV Graphics Controller, монитор: Proview 777(N) / 786(N) [17" CRT], клавиатура, мышь.); Foxconn G31MVP/G31MXP\DualCore Intel Pentium E2200\1 ГБ DDR2-800 DDR2 SDRAM\MAXTOR STM3160215A (160 ГБ, 7200 RPM, Ultra-ATA/100)\Optiarc DVD RW AD-7243S\Intel GMA 3100 монитор: acer v193w [19"], клавиатура, мышь.) с возможностью подключения к сети Интернет и обеспечения доступа в электронную информационно-образовательную среду Белгородского ГАУ; настенный плазменный телевизор SAMSUNG PS50C450B1 Black HD (диагональ 127 см); аудио-видео кабель HDMI.

3.2. Информационное обеспечение обучения

Перечень учебных изданий, Интернет-ресурсов, учебно-методической, дополнительной литературы

Основные источники:

1.Партыка Т. Л. **Информационная безопасность**: Учебное пособие / Партыка Т. Л., Попов И. И. - 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2016. - 432 с **http://znanium.com/bookread2.php?book=516806**
2.Партыка Т. Л. **Информационная безопасность** : учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-

М, 2018. — 432 с. — (Среднее профессиональное образование).
http://znanium.com/bookread2.php?book=915902

Дополнительные источники:

1.Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 416 с.
http://znanium.com/bookread2.php?book=549989

Интернет ресурсы:

1. http://www.iis.ru/glossary/ - русско-английский глоссарий по информатике
2. http://www.RusEdu.info - сайт посвящен информатике и ИКТ в образовании

Электронные периодические издания (журналы)

1. http://www.infosoc.iis.ru/
2. https://bijournal.hse.ru
3. http://jit.nsu.ru

Перечень электронных ресурсов, к которым обеспечивается доступ обучающихся.

1. Министерство образования и науки Российской Федерации. http://минобрнауки.рф
2. Информационная система "Единое окно доступа к образовательным ресурсам". http://window.edu.ru
3. Единая коллекция цифровых образовательных ресурсов. http://school-collection.edu.ru
4. Федеральный центр информационно-образовательных ресурсов. http://fcior.edu.ru
5. Электронные библиотечные системы и ресурсы. http://www.tih.kubsu.ru
6. Электронная библиотека Белгородского ГАУ. http://lib.belgau.edu.ru/
7. Электронная информационно-образовательная среда Белгородского ГАУ http://do.belgau.edu.ru
8. Расписание занятий. http://rasp.bsaa.edu.ru
9. Версия официального сайта Белгородского ГАУ для слабовидящих http://bsaa.edu.ru/sveden/#

Для обучающихся среди инвалидов и лиц с ограниченными возможностями здоровья организован доступ к информационным системам и информационно-телекоммуникационным сетям в течение всего учебного времени в компьютерных классах

Печатные периодические издания (журналы)

Экономика, статистика и информатика

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Освоенные умения: -применять программное обеспечение для защиты от несанкционированного доступа; -применять программное обеспечение для защиты от вирусного заражения компьютера; -зашифровывать и дешифровывать сообщения различными методами; -создавать открытый ключ и вырабатывать индивидуальный секретный ключ для документов с помощью программного обеспечения.	Коллоквиум, тест, подготовка реферата, решение кейс-задач, решение задач, экзамен
Усвоенные знания: -принципы системного подхода к защите информации; - основные понятия криптографии; - принципы передачи информации; - методы шифрования и дешифрования.	