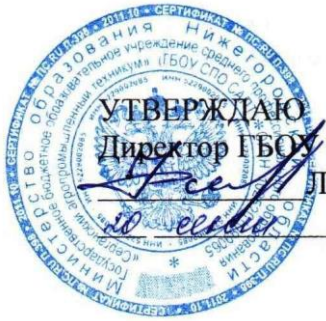
Государственное бюджетное образовательное учреждение
среднего профессионального образования
«Сергачский агропромышленный техникум»



УТВЕРЖДАЮ
Директор ГБОУ СПО САПТ
_____ Л.Г.Фокина
«20» сентября 2012 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.11 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Сергач – 2011 г.

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее ФГОС) по специальности среднего профессионального образования (далее СПО) **230701 Прикладная информатика (по отраслям)**, а так же на основе требований, предъявляемых работодателями.

Организация – разработчик: ГБОУ СПО «Сергачский агропромышленный техникум»

Разработчик: Юрин С.В. – преподаватель спец. дисциплин ГБОУ СПО «Сергачский агропромышленный техникум»

Рассмотрена На заседании МО ОПСД Протокол №1 от «28» сентября 2011 г. Руководитель МООПСД _____ Ташкинов А.А.	Утверждена Методическим советом ГБОУ СПО САПТ Протокол № от « »сентября 201 г. Методист _____ Моисеева Н.В.
Рассмотрена На заседании МО ОПСД Протокол №1 от «19» сентября 2012 г. Руководитель МООПСД _____ Ташкинов А.А.	Утверждена Методическим советом ГБОУ СПО САПТ Протокол № 1 от «20»сентября 2012 г. Методист _____ Моисеева Н.В.
Рассмотрена На заседании МО ОПСД Протокол №1 от «17» сентября 2013 г. Руководитель МООПСД _____ Ташкинов А.А.	Утверждена Методическим советом ГБОУ СПО САПТ Протокол № 1 от «20»сентября 2013 г. Методист _____ Моисеева Н.В.
Рассмотрена На заседании МО ОПСД Протокол № от « » сентября 201 г. Руководитель МООПСД _____ Ташкинов А.А.	Утверждена Методическим советом ГБОУ СПО САПТ Протокол № от « »сентября 201 г. Методист _____ Моисеева Н.В.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.11 Информационная безопасность

1.1.Область применения программы

Программа учебной дисциплины (далее программа) является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности (специальностям) СПО 230701 Прикладная информатика (по отраслям) (базовой подготовки)

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина входит в профессиональный цикл дисциплин вариативной части ФГОС СПО по специальности 230701 Прикладная информатика (по отраслям) (базовой подготовки).

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

В результате освоения дисциплины обучающийся должен **иметь представление**:

- об основных понятиях теории информации;
- о методах и средствах обеспечения информационной безопасности;
- о методах нарушения конфиденциальности целостности и доступности информации;
- об организации секретной связи с использованием криптосистем.

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

- содержание основных понятий обеспечения информационной безопасности;
- источники угроз безопасности информации;
- методы оценки уязвимости информации;
- методы создания, организации и обеспечения функционирования систем комплексной защиты информации;
- методы пресечения разглашения конфиденциальной информации;
- виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений.

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

- находить необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
- применять действующую законодательную базу в области информационной безопасности;
- разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации.

Содержание дисциплины ориентировано на подготовку студентов к освоению профессиональных модулей ОПОП по специальности 230701 «Прикладная информатика» и овладению **профессиональными компетенциями (ПК)**:

ПК 1.1 Обрабатывать статический информационный контент.
ПК 1.2 Обрабатывать динамический информационный контент.
ПК 2.1 Осуществлять сбор и анализ информации для определения потребностей клиента.
ПК 2.4 Проводить адаптацию отраслевого программного обеспечения

В процессе освоения дисциплины у студентов должны быть сформированы **общие компетенции**:

ОК1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес;
ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество;
ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность;
ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития;

ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности;
ОК6.Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями;
ОК7. Брать на себя ответственность за работу членов команды (починенных), за результат выполнения заданий;
ОК8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации;
ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

1.4. Количество часов на освоение программы дисциплины:

- максимальной учебной нагрузки обучающегося 135 часов, включая:
  - обязательной аудиторной учебной нагрузки обучающегося 90 часов, из них:
    – теоретических занятий 70 часов;
    – практических и лабораторных работ 20 часов;
  - самостоятельной работы обучающегося 45 часов.

2. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Тематический план и содержание учебной дисциплины «Информационная безопасность»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
Тема 1 Обеспечение информационной безопасности: содержание и структура	***Содержание учебного материала*** Понятие «обеспечение». Понятие «безопасность». Объект безопасности. Угрозы объекту безопасности.	2	1
	Обеспечение безопасности объекта. Понятие «информационная безопасность». Обеспечение информационной безопасности	2	
	Практическое занятие №1 *Концепции информационной безопасности*	2	2
	Самостоятельная работа обучающихся: Выполнение текущей домашней работы по теме «Обеспечение информационной безопасности: содержание и структура». Подготовка ответов на контрольные вопросы: 1. Что такое доступность информации? 2. Что такое конфиденциальная информация, государственная и коммерческая тайна? 3. Какие три возможные степени секретности вы знаете? 4. Каковы три категории ценности коммерческой информации? 5. Назовите основные методы определения объема информации.	3	3
Тема 2 Уязвимость информации в системах, обеспечивающих получение, сбор, хранение, передачу, обработку и отображение	***Содержание учебного материала*** Источники угроз безопасности информации.	2	1
	Системная классификация и общий анализ угроз.	2	
	Методы оценки уязвимости информации. Информационное оружие	2	
	Самостоятельная работа обучающихся: Выполнение текущей домашней работы по теме «Уязвимость информации в системах, обеспечивающих получение, сбор, хранение, передачу, обработку и отображение». Подготовка к практическому занятию с использованием методических рекомендаций преподавателя.	3	3
Тема 3 Основы теории информации	***Содержание учебного материала*** Понятие информации. Представление информации. Измерение информации.	2	1
	Эффективное кодирование информации. Передача информации	2	
	Практическое занятие №2 *Методы и средства защиты информации*	2	2
	Самостоятельная работа обучающихся: Выполнение текущей домашней работы по теме «Основы теории информации». Подготовка к практическому занятию с использованием	3	3

	методических рекомендаций преподавателя.		
Тема 4 Криптографические методы защиты информации	***Содержание учебного материала*** Исторический очерк развития криптографии.	2	1
	Основные понятия криптографии. Симметричные и ассиметричные шифрсистемы.	2	
	Организация секретной связи. Цифровая подпись.	2	
	Практическое занятие №3,4,5 *Криптографические методы защиты информации*	6	2
	Самостоятельная работа обучающихся: Выполнение текущей домашней работы по теме «Криптографические методы защиты информации». Оформление отчета по практической работе и подготовка к его защите. Составление кроссворда по теме «Криптографические методы защиты информации». Подготовка к практическому занятию с использованием методических рекомендаций преподавателя.	6	3
Тема 5 Защита информации от утечки по техническим каналам	***Содержание учебного материала*** Основные виды технических каналов и источников утечки информации.	2	1
	Способы предотвращения утечки информации по техническим каналам.	2	
	Практическое занятие №6 *Обеспечение безопасности компьютерных сетей*	2	2
	Самостоятельная работа обучающихся: Выполнение текущей домашней работы по теме «Защита информации от утечки по техническим каналам». Подготовка ответов на контрольные вопросы: 1. Что является предметом защиты в компьютерных сетях? 2. Перечислите основные правила безопасной работы КС 3. Чем обеспечивается целостность и доступность информации в КС? 4. Приведите основные методы и средства обеспечения ИБ в вычислительных сетях. 5. В чем заключается метод межсетевого экранирования?	3	3
Тема 6 Противодействие несанкционированному доступу к источникам конфиденциальной информации	***Содержание учебного материала*** Способы несанкционированного доступа. Технические средства несанкционированного доступа. Защита от наблюдения и фотографирования	2	1
	Защита от подслушивания. Противодействие незаконному подключению к каналам связи. Защита от перехвата.	2	
	Самостоятельная работа обучающихся: Выполнение текущей домашней работы по теме «Противодействие несанкционированному доступу к источникам конфиденциальной информации». Подготовка ответов на контрольные вопросы: 1. Опишите основные модели защиты объектов. 2. Какие средства оповещения и связи вам известны? Приведите их функциональную схему	2	3

	3. Приведите функциональные схема механической и оборонительной систем защиты.		
Тема 7 Законодательный уровень информационной безопасности	***Содержание учебного материала*** Что такое законодательный уровень информационной безопасности и почему он важен.	2	1
	Обзор российского законодательства в области информационной безопасности. Обзор зарубежного законодательства в области информационной безопасности.	2	
	О текущем состоянии российского законодательства в области информационной безопасности	2	
	Самостоятельная работа обучающихся: Выполнение текущей домашней работы по теме «Законодательный уровень информационной безопасности». Подготовка ответов на контрольные вопросы: 1. Что такое доктрина ИБ РФ? 2. Перечислите основные функции системы обеспечения ИБ РФ 3. Как подразделяются общие методы обеспечения ИБ РФ? 4. Перечислите внешние источники угроз ИБ РФ 5. Назовите внутренние источники угроз ИБ РФ	3	3
Тема 8 Программы-вирусы	***Содержание учебного материала*** Компьютерные вирусы как специальный класс саморепродуцирующих программ.	2	1
	Средства антивирусной защиты. Вирусное подавление как форма радиоэлектронной борьбы.	2	
	Самостоятельная работа обучающихся: Выполнение текущей домашней работы по теме «Программы-вирусы». Подготовка ответов на контрольные вопросы: 1. Каковы основные классификационные признаки компьютерных вирусов? 2. Приведите разновидности файловых вирусов. 3. Какие методы, средства и технологии борьбы с компьютерными вирусами вы знаете?	2	3
Тема 9 Стандарты и спецификации в области информационной безопасности	***Содержание учебного материала*** Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Основные понятия Механизм безопасности	2	1
	Классы безопасности Информационная безопасность распределенных систем. Рекомендации X.800 Сетевые сервисы безопасности Сетевые механизмы безопасности Администрирование средств безопасности	2	

	Стандарт ISO/IES 15408 «Критерий оценки безопасности информационных технологий» Основные понятия Функциональные требования Требования доверия безопасности Критерии европейских стран Интерпретация «Оранжевой книги» для сетевых конфигураций Руководящие документы Гостехкомиссии России	2	
	Самостоятельная работа обучающихся: Выполнение текущей домашней работы по теме «Стандарты и спецификации в области информационной безопасности». Подготовка к практическому занятию с использованием методических рекомендаций преподавателя.	3	3
Тема 10 Административный уровень информационной безопасности	***Содержание учебного материала*** Основные понятия. Политика безопасности. Программа безопасности.	2	1
	Синхронизация программы безопасности с жизненным циклом систем.	2	
	Практическое занятие №7 *Разработка алгоритма и программы кодирования с помощью методов распределения ключей*	2	2
	Самостоятельная работа обучающихся: Выполнение текущей домашней работы по теме «Административный уровень информационной безопасности». Подготовка обучающимися докладов. Примерные темы докладов: 1. BS 7799-1: 2005 – Британский стандарт BS 7799 первая часть; 2. BS 7799-2: 2005 - Британский стандарт BS 7799 вторая часть; 3. BS 7799-3: 2006 - Британский стандарт BS 7799 третья часть стандарта; 4. ISO/IEC 17799: 2005 – Международный стандарт, базирующийся на BS 7799 – 1: 2005; 5. ISO/IEC 27001: 2005 – Международный стандарт, базирующийся на BS 7799-2: 2005; 6. ISO/IEC 27005 – Руководство по менеджменту рисов ИБ; 7. ГОСТ Р 50922-2006 – Защита информации. Основные термины и определения.	3	3
Тема 11 Процедурный уровень информационной безопасности	***Содержание учебного материала*** Основные классы мер процедурного уровня Управление персоналом	2	1
	Физическая защита. Поддержание работоспособности	2	
	Реагирование на нарушения регента безопасности. Планирование восстановительных работ	2	
	Практическое занятие №8 *Разработка алгоритма и программы кодирования с помощью методов ЭЦП*	2	2
	Самостоятельная работа обучающихся:	4	3

	Выполнение текущей домашней работы по теме «Процедурный уровень информационной безопасности».		
Тема 12 Компьютерные преступления	***Содержание учебного материала*** Понятие компьютерных преступлений Криминалистическая характеристика компьютерных преступлений	2	1
	Способы совершения компьютерных преступлений Практика раскрытия и расследования компьютерных преступлений	2	
	Самостоятельная работа обучающихся: Выполнение текущей домашней работы по теме «Компьютерные преступления». Подготовка ответов на контрольные вопросы: 1. Какие основные эволюционные подходы к обеспечению ИБ деятельности общества вы знаете? 2. Приведите классификацию методов предотвращения угроз шпионажа и диверсий 3. Как классифицируют организационные и правовые методы и средства предотвращения угроз ИБ?	2	3
Тема 13 Пресечение разглашения конфиденциальной информации	***Содержание учебного материала*** Общие положения	2	1
	Характеристика пресечения разглашения	2	
	Аудит информационной безопасности	2	
	Самостоятельная работа обучающихся: Выполнение текущей домашней работы по теме «Пресечение разглашения конфиденциальной информации».	3	3
Тема 14 Комплексная система защиты информации	***Содержание учебного материала*** Концепция комплексной защиты информации Методология создания, организации и обеспечения	2	1
	Пути и проблемы практической реализации комплексной защиты информации	2	
	Перспективы комплексной защиты информации: защищенные информационные технологии	2	
	Практическое занятие №9,10 *Аппаратные и программные средства защиты компьютерной информации*	4	2
	Самостоятельная работа обучающихся: Выполнение текущей домашней работы по теме «Комплексная система защиты информации». Оформление отчета по практической работе и подготовка к его защите. Составление кроссворда по теме «Комплексная система защиты информации».	5	3
Экзамен			
Всего по дисциплине:		**90** **20**	

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 предполагает наличие учебной лаборатории «Информатика и компьютерная обработка информации. Теории информации. Операционные системы и среды. Информационные технологии»

Оборудование учебного кабинета:
- посадочные места по количеству обучающихся;
- рабочее место преподавателя.

Технические средства обучения:
- видеопроектор;
- компьютеры;
- программное обеспечение общего и специального назначения;
- интерактивная доска.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература:

1. Мельников В.П. Информационная безопасность : учеб. пособие для студ. учреждений сред. проф. образования / В.П.Мельников, С.А.Клейменов, А.М.Петраков ; под ред. С.А.Клейменова. – М. : Издательский центр «Академия», 2013. – 336 с.
2. Мельников В.П. Информационная безопасность : учеб. пособие для студ. учреждений сред. проф. образования / В.П.Мельников, С.А.Клейменов, А.М.Петраков ; под ред. С.А.Клейменова. – М. : Издательский центр «Академия», 2005. – 336 с.
3. А.А. Малюк, С.В. Пазизин, Н.С. Погожин Введение в защиту информации в автоматизированных системах: Учебное пособие.- М .: горячая линия – Телеком, 2004.-174 с.
4. Ярочкин В.И. Информационная безопасность.- М.: Академический проект, 2003.-639 с.
5. Галатенко В.А. Основы информационной безопасности: Курс лекций.- М.: Интернет-Университет Информационных технологий, 2003. – 239 с.
6. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос Ассоциация российских вузов, 2002. – 479 с.

Дополнительная литература:

1. Уфимцев Ю.С.и др. Методика информационной безопасности. – М.: Экзамен, 2004.- 543 с.
2. Копылов В. А.Информационное право : учебник/ В. А. Копылов; Моск. гос. юрид. академия. -2-е изд., перераб. и доп. -М.: ЮРИСТЪ, 2005 -512 с.

Базы данных, Интернет-ресурсы, информационно-справочные и поисковые системы

1. Архив учебных программ и презентаций RusEdu http://www.rusedu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	**Формируемые ОК**	**Формы и методы контроля и оценки результатов обучения**
Умения: *находить необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации*	*ОК 2 - ОК 9, ПК 1.1, ПК 2.1*	– *Устный опрос* – *Решение задач* – *Внеаудиторная самостоятельная работа.* – *Самостоятельная работа.* – *Тестирование* – *Собеседование* – *Групповые и индивидуальные практические работы* – *Наблюдение и оценка на практических занятиях при выполнении работ по изучаемой дисциплине* – *Оценка участия в исследовательской, научной работе* – *Контрольная работа* – *Экзамен*
применять действующую законодательную базу в области информационной безопасности	*ОК 2 - ОК 9, ПК 2.4*	
разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации	*ОК 2 - ОК9, ПК 1.1, ПК 1.2, ПК 2.1*	
Знания: *содержание основных понятий обеспечения информационной безопасности*	*ОК 1, ОК 4, ОК 9, ПК 1.1*	
источники угроз безопасности информации	*ОК 1, ОК 4, ОК 9, ПК 1.1, ПК 2.4*	
методы оценки уязвимости информации	*ОК 1, ОК 4, ОК 9, ПК 1.1, ПК 2.4*	
методы создания, организации и обеспечения функционирования систем комплексной защиты информации	*ОК 1, ОК 4, ОК 9, ПК 2.1, ПК 2.4*	
методы пресечения разглашения конфиденциальной информации	*ОК 1, ОК 4, ОК 9, ПК 1.2, ПК 2.1*	
виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений	*ОК 1, ОК 4, ОК 9, ПК 1.2*	