РЕСПУБЛИКА ТАТАРСТАН

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ

ГАОУ СПО «АЛЬМЕТЬЕВСКИЙ ПОЛИТЕХНИЧЕСКИЙ ТЕХНИКУМ»

РАБОЧАЯ ПРОГРАММА

по дисциплине	«Информационная безопасность»
для специальности	230105 Программное обеспечение вычислительной техники и автоматизированных систем.

2010

Одобрена на заседании
Цикловой комиссии
Протокол №__ от «__» _____2010г.
Председатель цикловой комиссии
_____М. А. Бондарева

Составлена в соответствии с Государственным стандартом среднего профессионального образования к минимуму содержания и уровня подготовки выпускников по специальности

УТВЕРЖДАЮ
Зам. директора по УР
_____Л. С. Мавлявеева
«___»_____ 2010

Составила	Куликова А. А.	преподаватель информационных дисциплин ГАОУ СПО «Альметьевский политехнический техникум»
Рецензент	Бондарева М. А.	преподаватель информационных дисциплин ГАОУ СПО «Альметьевский политехнический техникум»
Рецензент	Багута М. А.	заместитель главного энергетика ООО ТатБурМонтаж

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа учебной дисциплины «Информационная безопасность» предназначена для реализации государственных требований к минимуму содержания и уровню подготовки выпускников по специальности 230105 Программное обеспечение вычислительной техники и автоматизированных систем.

Учебная дисциплина «Информационная безопасность» является специальной, формирующей профессиональные знания, необходимые для будущей трудовой деятельности.

Дисциплина «Информационная безопасность» имеет практическую направленность и проводиться в тесной взаимосвязи с другими общепрофессиональными и специальными дисциплинами: «Операционные системы и среды», «Основы алгоритмизации и программирования», «Технические средства информатизации», «Базы данных», «Компьютерные сети», «Разработка и эксплуатация удаленных баз данных», «Технология разработки программных продуктов», «Программное обеспечение компьютерных сетей».

В результате изучения дисциплины **студент должен:**

иметь представление:

- о роли и месте знаний по дисциплине «Информационная безопасность» при освоении смежных дисциплин по выбранной специальности и в сфере профессиональной деятельности;

знать:

- источники возникновения информационных угроз;
- модели и принципы защиты информации от несанкционированного доступа;
- методы антивирусной защиты информации;
- состав и методы организационно-правовой защиты информации;

уметь:

- применять правовые, организационные, технические и программные средства защиты информации;
- создавать программные средства защиты информации.

Программа рассчитана на 80 часов аудиторных занятий, в том числе 20 часов отводится на практические занятия.

Для закрепления теоретических знаний и приобретения необходимых практических умений программой дисциплины предусматривается проведение практических занятий.

ТЕМАТИЧЕСКИЙ ПЛАН
УЧЕБНОЙ ДИСЦИПЛИНЫ

Наименование тем и разделов	Максим. учебная нагрузка	Количество аудиторных часов при очной форме обучения в том числе			Самостоят. работа
		лекции	Лаб. раб	Практ. занятия	
Введение	2	2			
Раздел 1. Борьба с угрозами несанкционированного доступа к информации	56	24		16	12
Тема 1.1. Актуальность проблемы обеспечения безопасности информации	12	8			4
Тема 1.2.Виды мер обеспечения информационной безопасности	24	10		10	4
Тема 1.3. Основные принципы построения систем защиты информации	20	10		6	4
Раздел 2 Борьба с вирусным заражением информации	30	18		4	8
Тема 2.1. Проблема вирусного заражения и структура современных вирусов	14	8		2	4
Тема 2.2 Классификация антивирусных программ	16	10		2	4
Раздел 3 Организационно-правовое обеспечение информационной безо-пасности	20	16			4
Тема 3.1. Международные, российские и отраслевые правовые документы	20	16			4
Всего по дисциплине	108	64		20	24

СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ВВЕДЕНИЕ

Студент должен:

иметь представление:

- о роли и месте знаний по дисциплине в сфере профессиональной деятельности;
- об основных проблемах и перспективах развития информационной безопасности.

Предмет и задачи информационной безопасности. Эволюция подходов к обеспечению информационной безопасности.

Раздел 1 БОРЬБА С УГРОЗАМИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

Тема 1.1 Актуальность проблемы обеспечения безопасности информации

Студент должен:

знать:

- виды объектов, подлежащих защите, и необходимость защиты информации;
- источники и пути реализации несанкционированного доступа к информации;
- классификация угроз информационной безопасности объектов.

Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации. Угрозы информационной безопасности: классификация, источники возникновения и пути реализации. Определение требований к уровню обеспечения информационной безопасности.

Тема 1.2 Виды мер обеспечения информационной безопасности

Студент должен:

знать:

- виды и назначение различных мер обеспечения информационной безопасности;

– особенности использования технических и программно-математических мер;

уметь:

– определять необходимый уровень безопасности информации;
– специфически управлять техническими средствами с целью пресечения несанкционированного доступа;
– создавать программные продукты по защите информации.

Практическое занятие №1. Аудит и журналы безопасности Windows;
Практическое занятие № 2. Изучение возможностей безопасности ПК;
Практическое занятие № 3. Основные возможности программы Expert 2.0;
Практическое занятие № 4. Управление правами пользователей в операционной системе Windows XP;
Практическое занятие № 5. Защита от несанкционированного доступа.

Виды мер обеспечения информационной безопасности: законодательные, морально-этические, организационные, технические, программно-математические. Специфические приемы управления техническими средствами. Методы защиты от копирования. Некопируемые метки. Защита от средств отладки и дисассемблирования. Защита от трассировки по заданному прерыванию. Защита программ в оперативной памяти. Механизмы защиты операционных систем. Системы защиты программного обеспечения. Защита информации в корпоративных сетях.

Тема 1.3 Основные принципы построения систем защиты информации

Студент должен:

знать:

– назначение и место использования идентификации и аутентификации;
– необходимость использования разграничения доступа;
– основные возможности криптографических методов защиты информации.

Основные защитные механизмы: идентификация и аутентификация. Разграничение доступа. Контроль целостности. Криптографические механизмы конфиденциальности, целостности и аутентичности информации. Обнаружение и противодействие атакам.

Практическое занятие №6. Перестановочный шифр;
Практическое занятие №7. Атака на алгоритм шифрования RSA посредством метода ферма;

Практическое занятие №8. Атака на алгоритм шифрования RSA методом бесключевого чтения.

Раздел 2 БОРЬБА С ВИРУСНЫМ ЗАРАЖЕНИЕМ ИНФОРМАЦИИ

Тема 2.1 Проблема вирусного заражения и структура современных вирусов

Студент должен:

знать:

- пути проникновения компьютерных вирусов;
- классификацию деструктивных воздействий вируса;
- средства защиты от воздействия вирусов;

уметь:

- распознавать воздействие вируса на программный продукт или данные;
- противодействовать вирусной атаке.

Практическое занятие № 9. Основные признаки присутствия на компьютере вредоносных программ.

Компьютерный вирус: понятие, пути распространения, проявление действия вируса. Структура современных вирусов: модели поведения вирусов; деструктивные действия вируса; разрушение программы защиты, схем контроля или изменение состояния программной среды; воздействия на программно-аппаратные средства защиты информации. Программы-шпионы. Взлом парольной защиты. Защита от воздействия вирусов.

Тема 2.2 Классификация антивирусных программ

Студент должен:

знать:

- виды и назначение антивирусных программ;
- методы профилактики заражения вирусами;

уметь:

- использовать антивирусные программы.

Практическое занятие № 10. Работа с Антивирусом Касперского.

Программы–детекторы, программы–доктора, программы–ревизоры, программы–фильтры. Профилактика заражения вирусом.

Раздел 3 ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 3.1 Международные, российские и отраслевые правовые документы

Студент должен:

знать:

- основные международные правовые акты по защите информации;
- основные положения и принципы международных соглашений;
- соответствие российских и международных правовых соглашений;
- российские общегосударственные правовые документы по защите информации;
- российские отраслевые нормативные документы по защите информации;
- назначение должностных инструкций;
- методы контроля за исполнением должностных инструкций.

Опыт законодательного регулирования информатизации в России и за рубежом. Концепция правового обеспечения информационной безопасности Российской Федерации. Стандарты и нормативно-методические документы в области обеспечения информационной безопасности. Государственная система обеспечения информационной безопасности. Международные правовые акты по защите информации. Состав и назначение должностных инструкций. Порядок создания, утверждения и исполнения должностных инструкций.

ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

№	Наименование тем	Наименование	Количество аудиторных часов
1	Тема 1.2	Аудит и журналы безопасности Windows	2
2	Тема 1.2	Изучение возможностей безопасности ПК	2
3	Тема 1.2	Основные возможности программы Expert 2.0.	2
4	Тема 1.2	Управление правами пользователей в операционной системе Windows XP	2
5	Тема 1.2	Защита от несанкционированного доступа	2
6	Тема 1.3	Перестановочный шифр.	2
7	Тема 1.3	Атака на алгоритм шифрования RSA посредством метода ферма	2
8	Тема 1.3	Атака на алгоритм шифрования RSA методом бесключевого чтения	2
9	Тема 2.2	Основные признаки присутствия на компьютере вредоносных программ	2
10	Тема 2.1	Работа с Антивирусом Касперского	2
		Итого	20

САМОСТОЯТЕЛЬНАЯ РАБОТА

Номер темы	Тема
Тема 1.1.	Информационное общество: особенности становления и развития
Тема 1.1.	Современные угрозы и каналы утечки информации в компьютерных сетях
Тема 1.2.	Физическая защита объектов
Тема 1.2.	Проблемы защиты информации в компьютерных сетях
Тема 1. 3.	Алгоритмы и ключи
Тема 1. 3.	Шифры
Тема 2.1.	Основы компьютерной вирусологии
Тема 2. 1.	Макровирусы
Тема 2. 2.	Разнообразие антивирусных программ
Тема 2. 2.	Компьютерные вирусы и борьба с ними
Тема 3. 1.	Меры правовой защиты ИБ. Основные документы различных стран мира
Тема 3. 1.	Единые стандарты информационной безопасности

ТЕХНИЧЕСКИЕ СРЕДСТВА

Компьютерный класс: компьютеры P-IV/512/60 – 15 шт, принтер HP LJ 5000.

Программное обеспечение: Windows XP, Expert 2.0, Антивирус Касперского.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Основная литература:

1. В. П. Мельников, С. А. Клейменов, А. М. Петраков «Информационная безопасность»
2. Т. Л. Партыка, И. И. Попов «Информационная безопасность»
3. И. Конев, А. Беляев «Информационная безопасность предприятия»
4. В. И. Ярочкин «Информационная безопасность: Учебник»

Дополнительная литература:

1. Скотт Бармен «Разработка правил информационной безопасности»
2. Н. Фергюсон, Б. Шнайер «Практическая криптография»