МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

«Воронежский государственный педагогический университет»

УТВЕРЖДАЮ
Проректор по учебной работе _____Г.П. Иванова

«____»_____20___г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

Уровень основной образовательной программы: *бакалавриат*

Направление подготовки: *230700, Прикладная информатика*
Профиль: *10 Прикладная информатика в образовании*
Форма обучения: *очная*
Срок освоения ООП: *4 года*
Кафедра: *информатики и методики преподавания математики*

Разработчик(и):

Доцент кафедры информатики и МПМ _____ А.С. Сидоров

Доцент кафедры информатики и МПМ _____ О.А. Сидорова

Начальник учебно-методического управления _____ Т.В. Майзель

Рабочая программа учебной дисциплины одобрена на заседании кафедры
от «_____» _____20___г. Протокол № _____

Заведующий кафедрой _____ А.С. Потапов

г. Воронеж – 2011 г.

Лист переутверждения рабочей программы учебной дисциплины

Рабочая программа:

одобрена на 20__/20__ учебный год. Протокол № ___ заседания кафедры

от “___”_____ 20___ г.

Ведущий преподаватель_____

Зав. кафедрой_____

одобрена на 20__/20__ учебный год. Протокол № ___ заседания кафедры

от “___”_____ 20___ г.

Ведущий преподаватель_____

Зав. кафедрой_____

одобрена на 20__/20__ учебный год. Протокол № ___ заседания кафедры

от “___”_____ 20___ г.

Ведущий преподаватель_____

Зав. кафедрой_____

одобрена на 20__/20__ учебный год. Протокол №___ заседания кафедры

от “___”_____ 20___ г.

Ведущий преподаватель_____

Зав. кафедрой_____

одобрена на 20__/20__ учебный год. Протокол № ___заседания кафедры

от “___”_____ 20___ г.

Ведущий преподаватель_____

Зав. кафедрой_____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины **«Информационная безопасность»**:

- познакомить студентов с основными понятиями и определениями информационной безопасности; источниками, рисками и формами атак на информацию; угрозами, которым подвергается информация;
- познакомить студентов с организацией работы вредоносных программ; защитой от компьютерных вирусов и других вредоносных программам; методами и средствами защиты информации; политикой безопасности компании в области информационной безопасности;
- познакомить студентов со стандартами информационной безопасности; криптографическими методами и алгоритмами шифрования информации; алгоритмами аутентификации пользователей; защитой информации в сетях; требованиям к системам защиты информации.

В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **компетенции**:

- способен использовать, обобщать и анализировать информацию, ставить цели и находить пути их достижения в условиях формирования и развития информационного общества (ОК-1);
- способен работать в коллективе, нести ответственность за поддержание партнерских, доверительных отношений (ОК-3);
- способен понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (ОК-13);
- способен оценивать и выбирать современные операционные среды и информационно-коммуникационные технологии для информатизации и автоматизации решения прикладных задач и создания ИС в образовательных системах (ПК-16);
- способен анализировать и выбирать методы и средства обеспечения информационной безопасности (ПК-18);
- способен анализировать рынок программно-технических средств, информационных продуктов и услуг для решения прикладных задач и создания информационных систем в образовательных системах (ПК-19).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

2.1. Учебная дисциплина **«Информационная безопасность»** относится к базовому уровню профессионального цикла.

2.2. Для изучения данной учебной дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: «Базы данных», «Информатика и программирование».

2.3. Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: «Управление информационными системами», «Информационные системы организации и управления учебным процессом»

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. В результате изучения учебной дисциплины **«Наименование дисциплины»** студенты овладевают следующими знаниями, умениями и навыками:

Знания:

- знает различные способы получения и обработки информации;
- знает базовые понятия политики безопасности;
- знает основные требования информационной безопасности в различных сферах человеческой деятельности;
- знаком с понятийным аппаратом исследуемой области;
- знает различные аспекты информационной безопасности;
- знает современные тенденции развития рынка информационных услуг.

Умения:

- умеет формально описать условие поставленной задачи;
- умеет анализировать техническое задание;
- умеет выбирать программное обеспечение для осуществления защиты информации;
- умеет использовать алгоритмы и программные средства в целях осуществления защиты информации;
- умеет формулировать основные принципы защиты компьютерных систем;
- способен разграничивать сферы применения программных продуктов.

Навыки:

- владеет базовыми навыками работы с информацией;
- владеет навыками по работе с сертификатами безопасности;
- владеет навыками поддержания работоспособности систем информационной безопасности;
- владеет навыками организации криптосистем;
- владеет навыками установки, настройки и использования средств защиты информации;
- реализует на практике полученные знания в рамках изучаемой предметной области.

3.2. Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

ОК-1: способен использовать, обобщать и анализировать информацию, ставить цели и находить пути их достижения в условиях формирования и развития информационного общества

Структура компетенции	**Основные признаки уровня**	
	Базовый уровень	**Повышенный уровень**
знает различные способы получения и	имеет представление о методах анализа информации	знает пути и методы поиска, использования и обобщения информации

обработки информации		
умеет формально описать условие поставленной задачи	умеет формулировать цели и задачи исследования	способен формулировать и конкретизировать цели и задачи исследования
владеет базовыми навыками работы с информацией	владеет понятийным аппаратом	владеет навыками обработки и переработки информации

ОК-3: способен работать в коллективе, нести ответственность за поддержание партнерских, доверительных отношений

Структура компетенции	**Основные признаки уровня**	
	Базовый уровень	**Повышенный уровень**
знает базовые понятия политики безопасности	имеет представление об основных понятиях (безопасность, информация и т.д.)	знает основные принципы по обеспечению информационной безопасности в коллективе
умеет анализировать техническое задание	умеет выполнять поставленные задачи для достижения коллективных целей	умеет формулировать перед каждым членом коллектива задачи для достижения общей цели обеспечения информационной безопасности
владеет навыками по работе с сертификатами безопасности	владеет базовыми навыками по организации безопасности на уровне отдельных ИС	владеет навыками по организации информационной безопасности на уровне сложных систем

ОК-13: способен понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны

Структура компетенции	**Основные признаки уровня**	
	Базовый уровень	**Повышенный уровень**
знает основные требования информационной безопасности в различных сферах	имеет представление об информации, ее видах;	имеет представление о структуре информации;
	дает определение основных понятий (информация, безопасность);	имеет представление о комплексе мер по защите информации на уровне пер-

человеческой деятельности	имеет представление о коммерческой и государственной тайне	сональных данных, компании, государства.
умеет выбирать программное обеспечение для осуществления защиты информации	умеет классифицировать информацию по степени важности;	использует различные средства по защите информации (архивация, антивирусная профилактика и т.д.)
	умеет использовать средства антивирусной защиты	
владеет навыками поддержания работоспособности систем информационной безопасности	владеет навыками работы с антивирусными пакетами;	владеет навыками по организации комплекса мер по защите информации
	владеет навыками превентивных мер защиты информации	

ПК-16: способен оценивать и выбирать современные операционные среды и информационно-коммуникационные технологии для информатизации и автоматизации решения прикладных задач и создания ИС в образовательных системах

Структура компетенции	**Основные признаки уровня**	
	Базовый уровень	**Повышенный уровень**
знаком с понятийным аппаратом исследуемой области	дает определение основных понятий (защита, вирус, авторское право и т.д.);	имеет представление об алгоритмах кодирования информации;
	имеет представление о способах защиты программного обеспечения от нелегального использования;	способен идентифицировать криптографические алгоритмы
	имеет представление о типах лицензий ПО	
умеет использовать алгоритмы и программные средства в целях осуществления защиты информации	умеет использовать специализированное ПО, предназначенное для защиты от нелегального копирования	разрабатывает программы, предназначенные для защиты авторского права
владеет навыками органи-	владеет методами кодирования информации	владеет навыками по разработке алгоритмов защиты информации

зации крипто-систем		

ПК-18: способен анализировать и выбирать методы и средства обеспечения информационной безопасности

Структура компетенции	**Основные признаки уровня**	
	Базовый уровень	**Повышенный уровень**
знает различные аспекты информационной безопасности	знает основные математические методы и принципы построения средств защиты информации	положения основных нормативных документов, регламентирующих деятельность в области защиты информации
	знает основные уязвимости, возникающие при защите компьютерных систем и факторы, влияющие на уровень защищенности	основные подходы к выявлению и предотвращению компьютерных атак
умеет формулировать основные принципы защиты компьютерных систем	получать качественные оценки защищенности компьютерных систем	умеет выявлять потенциальные уязвимости компьютерных систем
владеет навыками установки, настройки и использования средств защиты информации	владеет приемами и программными средствами выявления компьютерных атак	владеет навыками оценки уровня защищенности компьютерных систем

ПК-19: способен анализировать рынок программно-технических средств, информационных продуктов и услуг для решения прикладных задач и создания информационных систем в образовательных системах

Структура компетенции	**Основные признаки уровня**	
	Базовый уровень	**Повышенный уровень**
знает современные тенденции развития рынка информационных услуг	имеет представление о потребностях рынка в информационных продуктах	знает потребности рынка программных и информационных продуктов
способен разграничивать сферы применения про-	учитывает потребности рынка при разработке информационных продуктов	умеет применять на практике различные условия рынка программных продуктов

граммных продуктов		
реализует на практике полученные знания в рамках изучаемой предметной области	владеет базовыми навыками по разработке продуктов, учитывающих потребности рынка	владеет различными приемами по разработке ИС в образовательных системах в рамках изучаемого предмета

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. ОБЪЕМ УЧЕБНОЙ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы		**Всего часов**
		Д/О
Аудиторные занятия (всего)		54
В том числе:		
Лекции (Л)		18
Практические занятия (ПЗ), Семинары (С)		-
Лабораторные работы (ЛР)		36
Самостоятельная работа студента (СРС)		54
СРС в период промежуточной аттестации		-
Вид промежуточной аттестации	зачет (З)	3
	экзамен (Э)	-
ИТОГО: Общая трудоемкость	**часов**	108
	зач. ед.	3

4.2. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

4.2.1. Разделы дисциплины, виды учебной деятельности и формы контроля

№ п/п	**Наименование раздела учебной дисциплины**	**Виды учебной деятельности, включая самостоятельную работу студентов (в часах)**					**Форма текущего контроля**
		Л	**ЛР**	**ПЗ**	**СРС**	**всего**	
1.	Компьютерные вирусы	4	8	0	12	24	Тестирование
2.	Доступ к информации	6	12	0	18	36	Отчет по ЛР
3.	Изучение работы популярных антивирусных пакетов. Разработка алгоритмов шифрования и дешифрования информации	8	16	0	24	48	Отчет по ЛР, тестирование
4.	Итого	18	36	0	54	108	

4.2.2. Содержание разделов учебной дисциплины

№ п/п	Наименование раздела учебной дисциплины (модуля)	Содержание раздела в дидактических единицах
1.	Компьютерные вирусы	Способы распространения компьютерных вирусов. Антивирусные программы. Методы работы антивирусных программ
2.	Доступ к информации	Способы несанкционированного доступа к информации. Противодействие несанкционированному доступу. Общие сведения по классической криптографии и алгоритмам блочного шифрования. Электронная подпись
3.	Изучение работы популярных антивирусных пакетов. Разработка алгоритмов шифрования и дешифрования информации	Пакет PGP. Создание ключей. Импорт и экспорт открытого ключа. Кодирование информации при помощи PGP. Раскодирование информации при помощи PGP.

4.2.3. Образовательные технологии

№ п/п	Наименование раздела учебной дисциплины	Образовательные технологии
1.	Компьютерные вирусы	Вводная лекция, Ситуация-упражнение, технология учебного исследования
2.	Доступ к информации	Вводная лекция, лекция-информация, Ситуация-упражнение, технологии проблемного обучения, технология учебного исследования
3.	Изучение работы популярных антивирусных пакетов. Разработка алгоритмов шифрования и дешифрования информации	Вводная лекция, лекция-информация, занятие-практикум, технологии проблемного обучения, технология учебного исследования

___35_____% - интерактивных занятий от объема аудиторных занятий

4.2.4. Лабораторный практикум

№ п/п	Наименование раздела учебной дисциплины	Наименование лабораторных работ	Всего часов
1.	Компьютерные вирусы	Настройка антивирусной защиты	8
2.	Доступ к информации	Реализация типовых методов защиты от несанкционированного доступа	12
3.	Изучение работы популярных ан-	Анализ надежности антивирусных	16

	тивирусных пакетов. Разработка алгоритмов шифрования и дешифрования информации	пакетов. Работа с PGP	
	ИТОГО:		36

4.3. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТА

4.3.1. Планирование СРС

№ п/п	Наименование раздела учебной дисциплины	Виды СРС	Всего часов
1.	Компьютерные вирусы	Выполнение домашних заданий; подготовка к компьютерному и бланочному тестированию; выполнение индивидуальных заданий; поиск информации в сети Интернет	12
2.	Доступ к информации	консультации преподавателя; работа над проектами; поиск информации в сети Интернет	18
3.	Изучение работы популярных антивирусных пакетов. Разработка алгоритмов шифрования и дешифрования информации	подготовка ответов на вопросы лекционного материала; подготовка отчета по ЛР; консультации преподавателя; работа над проектами	24

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ УСПЕВАЕМОСТИ И РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

5.1. Текущий контроль

В ходе текущего контроля оцениваются достижения студентов в процессе освоения дисциплины. Текущий контроль включает оценку самостоятельной (внеаудиторной) и аудиторной работы (в том числе рубежный контроль). В качестве оценочных средств используются: отчеты по лабораторным работам; компьютерное и бланочное тестирование; индивидуальные домашние задания, творческие работы, проекты.

5.2. Промежуточная аттестация по дисциплине

Промежуточная аттестация студентов по дисциплине предполагает зачет, который проводится в соответствии с «Положением о проведении текущего контроля успеваемости и промежуточной аттестации студентов ВГПУ».

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

6.1. Основная литература

1. Милославская Н. Г., Толстой А. Г. Интрасети: доступ в Internet, защита.- М.: ЮНИТА-ДАНА, 2000
2. Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий.- СПб.: BHV, 2000.
3. Соколов А. В., Степанюк О. М. Методы информационной защиты объектов и компьютерных сетей.- М.: АСТ, 2000.

6.2. Дополнительная литература

1. Пауэрс Л., Снелл М. Microsoft Visual Studio 2008. — СПб.: «БХВ-Петербург», 2008. — 1200 с.
4. Нил Дж. Рубенкинг. Язык программирования Delphi для «чайников». Введение в Borland Delphi 2006. — М.: Диалектика, 2007. — 336 с.

6.3. Программное обеспечение и Интернет-ресурсы:
Delphi, Visual Studio.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

7.1. Требования к аудиториям (помещениям, местам) для проведения занятий:
Стандартно оборудованная лекционная аудитория для проведения интерактивных лекций: видеопроектор, экран настенный, др. оборудование.
Компьютерный класс для проведения лабораторных работ

7.2. Требования к оборудованию рабочих мест преподавателя и обучающихся:
В компьютерном классе должны быть установлены: Visual Studio, Borland Delphi.