Белорусский государственный университет

УТВЕРЖДАЮ

Проректор по учебной работе

_____ А.В. Данильченко

_____2013г.

Регистрационный № УД-____/р.

Информационная безопасность

Учебная программа учреждения высшего образования по учебной дисциплине для специальности:

1-25 01 02 экономика

(код специальности) (наименование специальности)

Факультет Экономический

Кафедра Экономической информатики

(название кафедры)

Курс (курсы) 1

Семестр (семестры) 2

Лекции 26

Экзамен

Практические (семинарские) занятия 28

Зачет 2

Лабораторные занятия

Курсовая работа (проект)

Аудиторных часов по учебной дисциплине 54

Всего часов по учебной дисциплине 116

Форма получения высшего образования очное

Составил(а) О.В. Дубровина

2013 г.

Рассмотрена и рекомендована к утверждению кафедрой
экономической информатики

_____
(дата, номер протокола)

Заведующий кафедрой
_____ А.А.Королева

Одобрена и рекомендована к утверждению
Учебно-методической комиссией экономического факультета
(название учреждения высшего образования)

_____
(дата, номер протокола)

Председатель
_____ Е.Э.Васильева

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа «Информационная безопасность» разработана для студентов 1 курса специальности 1-25 01 02 «Экономика».

Базой для изучения данного курса являются дисциплины «Высшая математика», «Компьютерные информационные технологии», изучаемые в предыдущих семестрах.

Дисциплина «Информационная безопасность» имеет профессиональную и общенаучную направленность. Целью настоящего курса является ознакомление студентов с методологическими и организационными основам защиты информации, а также с особенностями применения специализированных программных средств для организации защиты корпоративной и личной информации при использовании компьютерных средств и сетей.

. При преподавании данной дисциплины ставятся следующие задачи:

- сформулировать основные задачи и методы защиты информации;
- ознакомить студентов с принципами формирования политики информационной безопасности;
- изучить механизмы информационной безопасности;
- ознакомить студентов с криптографическими методами защиты информации;
- ознакомить студентов с принципами работы компьютерных вирусов и современного антивирусного программного обеспечения;
- ознакомить студентов с моделями безопасного поведения в сети Интернет и социальных сетях.

«Информационная безопасность» является непосредственно связана с основными дисциплинами аналитического цикла, такими как «Компьютерные информационные технологии», «Информационные системы в экономике». При изложении курса важно как показать теоретические основы защиты информации, так и методы решения возникающих проблем на прикладном уровне.

В результате освоения курса «Алгебра и теория чисел» студент должен:

знать:

- основные определения защиты информации;
- механизмы защиты информации;
- примеры криптографических алгоритмов;
- основы векторной алгебры;

уметь:

- оценивать безопасность информационной системы;
- разрабатывать простейшую политику безопасности;
- применять криптографические системы на практике;
- использовать специализированное программное обеспечение;

приобрести навыки:

– применения методов защиты информации в профессиональной сфере и использование безопасной модели поведения в информационной среде и сети Интернет.

Изучение курса «Информационная безопасность» рассчитано на 116 часа, в том числе 54 часа аудиторных занятий.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1.

Тема 1. *Проблемы информационной безопасности.*

Современное состояние, перспектива и ретроспектива. Информационные системы, средства, каналы, сети и среды. Основные понятия и определения информационной безопасности. Информационные угрозы. Информационные атаки. Технические каналы утечки информации. Основные задачи защиты информации.

Тема 2. *Политика информационной безопасности.*

Административный уровень информационной безопасности. Политика безопасности. Программа безопасности. Процедурный уровень информационной безопасности. Организационное и правовое обеспечение информационной безопасности. Международные и отечественные правовые и нормативные акты обеспечения ИБ процессов переработки информации.

Тема 3. *Механизмы информационной безопасности.*

Идентификация, аутентификация. Биометрическая аутентификация Управление доступом. Организация управления доступом в компьютерной системе. Протоколирование и аудит.

Раздел 2.

Тема 1. *Общие принципы криптозащиты. Примеры алгоритмов шифрования.*

Классификация алгоритмов шифрования. Классификация угроз. Понятие стойкости алгоритма. Необходимые сведения булевой алгебры и теории чисел.

Простейшие алгоритмы шифрования.

Тема 2. *Контроль целостности данных.*

Общие сведения. Целостность данных. Типы функций хэширования. Примеры функций хэширования. Вопросы стойкости.

Общие положения электронной цифровой подписи. Примеры электронной цифровой подписи на основе алгоритмов с открытыми ключами.

Тема 3. *Стеганографические методы защиты информации.*

Математические понятия. Скрытие данных в неподвижных изображениях. Скрытие данных в текстовых файлах.

Раздел 3.

Тема 1. *Программная защита информации*.

Организация парольной защиты. Программно-аппаратные средства обеспечения информационной безопастности в вычислительных сетях. Защита документов. Контроль целостности. Защита от копирования. Защита от исследования. Защита от угроз нарушения доступности. Межсетевые экраны. Обеспечение безопасной работы современных операционных систем.

Тема 2. *Компьютерные вирусы. и антивирусное программное обеспечение*

Защита программного обеспечения от вирусного заражения, разрушающих программных действий и изменений. Компьютерные вирусы. Антивирусное программное обеспечение. Принципы работы, примеры.

Тема 3. *Безопасность сети Интернет.*

Организация защиты собственных ресурсов и конфиденциальной личной информации при использовании сети Интернет, социальных сетях, средствах коммуникации.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ
(ПРИМЕРНАЯ ФОРМА)

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов						Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Управляемая самостоятельная работа	Иное	
1	2	3	4	5	6	7	8	9
1	***Методологическое обеспечение информационной безопасности***	***6***	***6***			***30***		коллоквиум
1.1	Проблемы информационной безопасности.	2	2			10		
1.2	Политика информационной безопасности	2	2			10		
1.3	Механизмы информационной безопасности	2	2			10		
2	***Криптографические методы защиты информации***	***10***	***14***			***48***		письменный опрос
2.1	Общие принципы криптозащиты. Примеры алгоритмов шифрования	4	8			24		
2.2	Контроль целостности данных.	4	2			12		
2.3	Стеганографические методы защиты информации	2	4			12		
3	***Защита программ и данных***	***10***	***8***			***38***		коллоквиум
3.1	Программная защита информации	2	2			10		
3.2	Компьютерные вирусы и антивирусное программное обеспечение	4	2			14		
3.3	Безопасность сети Интернет	4	4			14		

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ОСНОВНАЯ ЛИТЕРАТУРА

1. Галатенко В.А. Основы информационной безопасности. Интернет-университет информационных технологий. – ИНТУИТ. ру, 2008.
2. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. – М., Академия, 2013.
3. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации. – М.: Академия, 2007.
4. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М: ДМК, 2000.
5. Харин Ю.С., Берник В.И., Матвеев Г.В. Математические основы криптологии. – Мн: БГУ, 2003.
6. Doubrovina O., Mityushev V., Rylko N. Rodstawy Bespieczeństwa Informatycznego. Inst. Matematyki Universitetu Pedagogicznego, Kraków, 2010.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

1. Шаньгин В., Защита компьютерной информации. – М.: ДМК, 2008.
2. С. Запечников. Информационная безопасность открытых систем. – М.: Горячая линия-Телеком, 2006.
3. Молдовян А. А., Молдовян Н. А., Советов Б. Я. Криптография. – СПб.: Лань, 2000.
4. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. – М.: Высшая школа, 1999.
5. Ященко В.В. Введение в криптографию. – М.: МЦНМО-ЧеРо, 1999.
6. Цырлов В.Л. Основы информационной безопасности. Ростов-на-Дону: Феникс, 2008.

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СРЕДСТВ ДИАГНОСТИКИ РЕЗУЛЬТАТОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ

Оценка промежуточных учебных достижений студента осуществляется по десятибалльной шкале.

Для оценки достижений студента используется следующий диагностический инструментарий:

– защита выполненных на практических занятиях индивидуальных заданий;

– выступление с докладом по отдельным темам;

– проведение текущих контрольных опросов по отдельным темам;

– проведение контрольных работ по отдельным темам

– сдача зачета.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ТЕМ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

1. Проблемы информационной безопасности. Оценка угроз.
2. Политика информационной безопасности. Программа информационной безопасности. Механизмы обеспечения безопасности.
3. Криптографические методы защиты информации. Примеры простейших алгоритмов шифрования.
4. Обеспечение целостности информации. Хэш-функции и электронная цифровая подпись.
5. Конфиденциальность данных. Парольная защита информации.
6. Компьютерные вирусы и антивирусное программное обеспечение.
7. Безопасное поведение в сети Интернет и социальных сетях.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ
(примерная форма)

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
1.			

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ
на _____/_____ учебный год

№№ пп	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (протокол № ____ от _____ 201_ г.)
(название кафедры)

Заведующий кафедрой

_____ _____ _____
(ученая степень, ученое звание) (подпись) (И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета

_____ _____ _____
(ученая степень, ученое звание) (подпись) (И.О.Фамилия)