

Учреждение образования "Гомельский государственный  
технический университет имени П.О. Сухого"

УТВЕРЖДАЮ  
Первый проректор  
УО «ГГТУ им. П.О. Сухого»

"25" 06 2012

Регистрационный № УДг-148-3/р

"ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ"

УЧЕБНАЯ ПРОГРАММА

для специальности 1 - 40 01 02 "Информационные системы и технологии  
(по направлениям)",  
направление специальности 1 - 40 01 02 - 01 "Информационные системы и  
технологии( в проектировании и производстве)"

Факультет

ФАИС

Кафедра

Информационные технологии

Курс 5

Семестр 9

Лекции 16 часа

Практические  
занятия —

Зачет 9 семестр

Лабораторные  
занятия 16 часов

Всего аудиторных часов  
по дисциплине 32

Всего часов  
по дисциплине 60

Форма получения  
высшего образования дневная

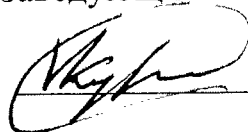
Программу разработали: заведующий кафедрой К.С.Курочка и ассистент  
Н.Н.Масалитина

Учебная программа составлена на основе учебной программы по курсу  
«Защита компьютерной информации» №УД- 624/уч. , утвержденной  
15.06.2012 УО «ГГТУ имени П.О.Сухого»

Рассмотрена и рекомендована к утверждению на заседании кафедры  
«Информационные технологии», протокол № 1.3

" 14 " мая 2012

Заведующий кафедрой

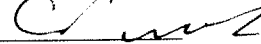


К.С. Курочка

Одобрена и рекомендована к утверждению научно-методическим советом  
ФАИС

«25» 06 2012

Протокол № 12

Председатель 

(ф.и.о., подпись)

## 1. Пояснительная записка

### 1.1. Цели и задачи учебной дисциплины

Курс «Защита компьютерной информации» является одним из основных при подготовке специалистов в области информационных технологий.

Цель курса «Защита компьютерной информации» - формирование у студентов навыков построения и использования математических моделей физических систем с применением информационных технологий.

Задачи изучения настоящей дисциплины состоят в следующем:

- Освоение навыков выявления угроз информационной безопасности;
- изучение методов криптографической защиты информации;
- изучение методов, идентификации и аутентификации пользователя;
- изучение законодательных и административных норм защиты информации;
- ознакомление с основными организационными методами защиты информации;
- получение навыков построения комплексной системы защиты информации от несанкционированного доступа и повреждения.

### 1.2. Требования к знаниям и умениям студентов после изучения дисциплины

После изучения данного курса студент должен:

- 1) уметь выявлять угрозы компьютерной информации и выбирать наиболее эффективные методы защиты от них;
- 2) знать и уметь использовать основные методы криптографии и криптологии;
- 3) иметь навыки построения комплексной системы защиты информации;
- 4) уметь оценивать эффективность существующей системы защиты информации и разрабатывать меры по ее улучшению.

### 1.3. Общее количество часов и распределение аудиторного времени по видам занятий.

Всего часов по дисциплине – 60, всего аудиторных часов – 32, из них лекций – 16 часов, лабораторных занятий – 16 часов.

## 2. Содержание учебного материала

### 2.1. Лекционные занятия

№ пп	Название темы, содержание	Объем в часах
1.	История и перспективы развития систем защиты информации	2
2.	Системная методология защиты информации	2
3.	Симметричные криптосистемы	2
4.	Асимметричные криптосистемы	4
5.	Идентификация пользователей кс-субъектов доступа к данным	2
6.	Механизм цифровой подписи	2
7.	Правовые и организационно-технические аспекты защиты информации	2
Итого:		16

### 2.2. Лабораторные занятия

№ пп	Название темы, содержание	Объем в часах
1.	Криптоанализ классических шифров	2
2.	Маршрутные и подстановочные шифры	3
3.	Шифрование, дешифрование информации с применением криптографических алгоритмов гаммирования	3
4.	Алгоритм шифрования данных DES	2
5.	Исследование ассиметричных алгоритмов шифрования	2
6.	Исследование методов идентификация и аутентификация пользователя	2
7.	Формирование и проверка электронной цифровой подписи на основе ассиметричного алгоритма RSA	2
Итого:		16

### 3. Учебно-методическая карта дисциплины

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов			самостоятельная работа студентов	Материальное обеспечение занятия (наглядные, методические пособия и др.)	Литература	Формы контроля знаний
		лекции	практические занятия	лабор. занят.				
1	2	3	4	5	6	7	8	9
1.	История и перспективы развития систем защиты информации	2		2	4	Компьютерная презентация № 1	КЛ, [1, 4, 7, 10]	3, О, ЗЛР
2.	Системная методология защиты информации	2			4	Компьютерная презентация № 2	КЛ, [4, 10]	3, О, ЗЛР
3.	Симметричные криптосистемы	2		6	4	Компьютерная презентация № 3	КЛ, [1, 5, 10]	3, О, ЗЛР
4.	Асимметричные криптосистемы	2		4	4	Компьютерная презентация № 4	КЛ, [1, 4, 5, 10]	3, О, ЗЛР
5.	Идентификация пользователей кс-субъектов доступа к данным	4		2	4	Компьютерная презентация № 5	КЛ, [3, 8, 10]	3, О, ЗЛР
6.	Механизм цифровой подписи	2		2	4	Компьютерная презентация № 6	КЛ, [4, 10]	3, О, ЗЛР
7.	Правовые и организационно-технические аспекты защиты информации	2			4	Компьютерная презентация № 7	КЛ, [2, 5, 6, 9, 10, 11]	3, О, ЗЛР

Принятые обозначения: КЛ- конспект лекций, О- отчет по лабораторной работе; ЗЛР- защита лабораторной работы; 3- зачет.

## 4. Информационно-методическая часть

### 4.1. Основная литература

1. Анин Б. Ю. Защита компьютерной информации – Санкт-Петербург :БХВ-Петербург, 2000. - 376с
2. Бузов Г.А. Защита от утечки информации по техническим каналам: учеб. пособие –Москва :Горячая линия-Телеком, 2005. - 414с
3. Мельников В. П. Информационная безопасность и защита информации: учебное пособие для вузов /В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова: учебное пособие для вузов – Москва :Академия, 2009. - 331 с
4. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства: учеб. пособие для вузов – Москва: ДМК, 2008. - 542 с.

### 4.2. Дополнительная литература

5. Об информации, информатизации и защите информации: закон Респ. Беларусь от 10 нояб. 2008г., № 455-З:закон Респ. Беларусь от 10 нояб. 2008г., № 455-З //Нац. реестр правовых актов Респ. Беларусь. – 2008. – № 279. - С. 14-27.
6. О некоторых вопросах защиты информации: пост. Совета Министров Респ. Беларусь от 26 мая 2009 г., № 675:пост. Совета Министров Респ. Беларусь от 26 мая 2009 г., № 675 //Нац. реестр правовых актов Респ. Беларусь. – 2009. – № 136. - С. 63-76.
7. Защита информации в системах мобильной связи: учеб. пособие для вузов /А. А. Чекалин [и др.]:учеб. пособие для вузов –Москва :Горячая линия-Телеком, 2005.
8. Ишейнов В.Я. Защита конфиденциальной информации: учебное пособие для вузов /В. Я. Ишейнов, М. В. Мещатунян – Москва :Форум, 2009. -254 с
9. Организация и современные методы защиты информации: Метод.пособие для руковод. и сотрудников служб безопасности /Агеев А.С.,Борисов с.а.,Диев С.А.и др.; Под общ.ред.С.А.Диева, А.Г.Шаваева – М. :Банковский Деловой Центр, 1998. - 472с.
10. Петраков А.В. Защита и охрана личности, собственности, информации: Справочное пособие: – М. :Радио и связь, 1997. -320с.
11. Технические средства и методы защиты информации: учебное пособие для вузов /А. П. Зайцев [и др.]; под ред. А. П. Зайцева, А. А. Шелупанова: – Москва :Горячая линия-Телеком, 2009. -614, [1] с.

Список литературы сверен *Проф. Лахманова Т.С.*

5. Протокол согласования учебной программы по изучаемой учебной дисциплине с другими дисциплинами специальности

Данная дисциплина не требует согласования с другими дисциплинами.

Зав.кафедрой ИТ



К.С.Курочка