МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ
(ТГПУ)

«УТВЕРЖДАЮ»
Декан физико-математического
факультета

_____ Е.Г. Пьяных

«27» мая 2015 года

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б.3.В.27 ОСНОВЫ КРИПТОГРАФИИ

ТРУДОЁМКОСТЬ (В ЗАЧЁТНЫХ ЕДИНИЦАХ) 4

Направление подготовки 050100.62 – Педагогическое образование

Профиль подготовки: Информатика и Математика

Квалификация (степень) выпускника бакалавр

1. Цели изучения дисциплины:

1.1. *Цели*:

Цель преподавания дисциплины – ознакомление студентов с методами криптографии и защиты данных.

1.2. *Задачи*:

Задача изучения дисциплины – привить навыки использования современных методов защиты данных.

2. Место учебной дисциплины в структуре основной образовательной программы.

Данная дисциплина относится к вариативной части профессионального цикла. Она является неотъемлемой частью профессионального образования студента.

Для освоения данной дисциплины требуются математические знания, полученные в ходе изучения следующих дисциплин: «Программирование», «Математика», «Информатика», «Теоретические основы прикладной математики и информатики».

3. Требования к уровню освоения содержания дисциплины

Компетенции, формируемые в рамках дисциплины «Трансляция с языков высокого уровня»:

владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения (ОК-1);

способность использовать знания о современной естественнонаучной картине мира в образовательной и профессиональной деятельности, применять методы математической обработки информации, теоретического и экспериментального исследования (ОК-4);

осознание социальной значимости своей будущей профессии, обладание мотивацией к осуществлению профессиональной деятельности (ОПК-1);

способность разрабатывать и реализовывать учебные программы базовых и элективных курсов в различных образовательных учреждениях (ПК-1);

способностью решать задачи воспитания и духовно-нравственного развития (ПК-2);

готовность использовать систематизированные теоретические и практические знания для определения и решения исследовательских задач в области образования (ПК-11);

способность использовать в учебно-воспитательной деятельности основные методы научного исследования (ПК-13).

В результате изучения дисциплины студент должен

знать основные алгоритмы ;

уметь применять их в практической деятельности;

владеть методами разработки эффективных алгоритмов

4. Общая трудоемкость дисциплины 4 зачётных единицы и виды учебной работы.

Вид учебной работы	Трудоемкость (в соответствии с учебным планом) (час)	Распределение по семестрам (в соответствии с учебным планом) (час)		
	144	6		
Аудиторные занятия	44 (в том числе в интера. – 10)	44 (в том числе в интера. – 10)		
Лекции				
Практические занятия	44	44		
Семинары				
Лабораторные работы				
Другие виды аудиторных работ				
Другие виды работы				
Самостоятельная работа	73	73		
Курсовой проект (работа)				
Реферат				
Расчетно-графические работы				
Формы текущего контроля				
Формы промежуточной аттестации в соответствии с учебным планом	27 (экзамен)	27 (экзамен)		

5. Содержание учебной дисциплины

5.1. Разделы учебной дисциплины

№ п/п	Наименование раздела дисциплины (темы)	Аудиторные часы					
		Всего	Лекции	Практ. (семинары)	Лабор. работы	В т.ч. интерактивные формы обучения (не менее 10%)	Сам. работа
1.	Кодирование информации.	4			4		15
2.	Несимметрические методы шифрования	10			10	6	15
3.	Симметрические методы шифрования.	14			14	4	15
4.	Электронная подпись.	8			8		15
5.	Защита данных в информационных системах.	8			8		15
ИТОГО:		44/ 1,2 зач.ед.			44	10 / 22,7%	73

5.2. Содержание разделов учебной дисциплины

1. Кодирование информации.

Кодирование ансамбля источника. Информация и энтропия. Теорема Шеннона. Сживающее кодирование. Шифрование.

2. Симметрические методы шифрования.

Простейшие методы шифрования. Код Цезаря. Методы подстановок и перестановок. Использование xor. Основные принципы шифрования с секретным ключом. Недостатки симметричных методов.

3. Несимметрические методы шифрования.

Односторонние функции и хеш-значения. Хранение авторизационных данных и алгоритм авторизации. Простейший метод шифрования с открытым ключом. Теорема Ферма и метод Ферма. Теорема Эйлера и метод RSA.

4. Электронная подпись.

Применение несимметрических методов для идентификации отправителя. Понятие электронной подписи. Центры сертификации.

5. Защита данных в информационных системах.

Основные методы защиты данных. Репликация. Защита данных в web-системах. sql-инъекции. Защищенные каналы связи. Использование PGP. Защита данных в операционных системах.

5.3. Лабораторный практикум

Не предусмотрен

6. Учебно-методическое обеспечение дисциплины

6.1. Основная литература по дисциплине:

1. Бабаш, А. В.. Информационная безопасность: лабораторный практикум : учебное пособие/А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников.-Москва:КНОРУС,2012.-131 с.

6.2. Дополнительная литература:

1. Шеннон, К. Теория связи в секретных системах. По изданию Клод Шеннон. "Работы по теории информации и кибернетике", М., ИЛ, 1963, с. 333-.
2. Жельников, В. Криптография от папируса до компьютера. - М.: ABF, 2008. – 335с. М.Левин. Криптография. Руководство пользователя. М.: Познавательная книга+, 2001.
3. Молдовян, А.А., Молдовян, Н.А., Советов, Б.Я. Криптография. – СПб.: Лань, 2010.

6.3. Средства обеспечения освоения дисциплины

В процессе изучения дисциплины, студент работает с многочисленными информационными источникам в сети Интернет.

В качестве примеров ссылок на интернет-источники можно привести:

http://intuit.ru

http://lib.ru

6.4. Материально-техническое обеспечение дисциплины

№ п/п	Наименование раздела (темы) учебной дисциплины	Наименование материалов обучения, пакетов программного обеспечения	Наименование технических и аудиовизуальных средств, используемых с целью демонстрации материалов
1	1, 2, 3,4,5,	Free Pascal, Free Pascal Lazarus, Borland Delphi или иной компилятор с языков Паскаль или С	Мультимедийный компьютерный класс, интерактивная доска, наличие локальной и глобальной сети.

7. Методические рекомендации по организации изучения дисциплины

7.1. Методические рекомендации преподавателю

Преподаватель должен последовательно излагать теоретический материал в рамках лекционных занятий. При этом предлагаемого материала должно быть достаточно для того, чтобы студент мог самостоятельно углублять полученные знания по мере необходимости. Важно помнить, что данная дисциплина, с одной стороны носит фундаментальный характер, так в ней достаточно подробно рассматривается теория формальных языков, с другой стороны дисциплина направлена на решение прикладных задач – построение трансляторов с языков высокого уровня различных типов.

На экзамене преподаватель должен убедиться не только в знании студентом вопросов конкретного билета, но и убедиться в общих знаниях по предмету. С этой целью могут непосредственно на экзамене задаваться дополнительные вопросы. При выставлении оценки, преподаватель должен ориентироваться не столько на объем информации, которую студент может «запомнить», сколько на «понимание» материала и способность к его практическому применению.

7.2. Методические рекомендации для студентов

Студентам предлагается использовать предлагаемый курс лекций, а также основную и дополнительную литературу для изучения предмета.

В рамках самостоятельной работы необходимо подготовить список вопросов по предлагаемым на обсуждение темам, выполнить задания, предлагаемые для самостоятельной работы, пройти тестирование по индивидуальному тесту, выдаваемому преподавателем.

Подготовка к обсуждению и дискуссиям оценивается по следующим критериям:

1) количество использованных источников;

2) актуальность предложенных на обсуждение вопросов;

3) активность, проявленная студентом при обсуждении;

4) аналитические способности, продемонстрированные при формулировании выводов и подведении результатов обсуждения.

8. Формы текущего контроля успеваемости и промежуточной аттестации обучающихся.

Вопросы и задания для самостоятельной работы.

1. Шифрование с секретным ключом.
2. Шифрование с открытым ключом.
3. Электронная подпись и ее применение.
4. Использование PGP.

Перечень вопросов для промежуточной аттестации (к экзамену).

1. Кодирование ансамбля источника.
2. Информация и энтропия.
3. Теорема Шеннона.
4. Сживающее кодирование.
5. Простейшие методы шифрования.
6. Код Цезаря. Методы подстановок и перестановок. Использование xor.
7. Основные принципы шифрования с секретным ключом.
8. Недостатки симметричных методов шифрования.
9. Односторонние функции и хеш-значения.
10. Хранение авторизационных данных и алгоритм авторизации.
11. Простейший метод шифрования с открытым ключом.
12. Теорема Ферма и метод Ферма.
13. Теорема Эйлера и метод RSA.
14. Применение несимметрических методов для идентификации отправителя.
15. Понятие электронной подписи. Центры сертификации.
16. Репликация и ее применение. Защита данных в web-системах.
17. Защищенные каналы связи.
18. sql-инъекции.
19. Использование PGP.
20. Защита данных в операционных системах.

Рабочая программа учебной дисциплины составлена в соответствии с учебным планом, федеральным государственным образовательным стандартом высшего профессионального образования по направлению подготовки: **050100.62 – Педагогическое образование**

Рабочая программа учебной дисциплины составлена:

Кандидат технических наук,
доцент кафедры информатики _____ А.Н. Стась

Рабочая программа учебной дисциплины утверждена на заседании кафедры информатики
протокол № 1 от «31» августа 2015 г.

Зав. кафедрой _____ А.Н. Стась

Рабочая программа учебной дисциплины одобрена методической комиссией физико-математического факультета
протокол № 1 от «31» августа 2015 г.

Председатель методической комиссии _____ З.А. Скрипко