МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Томский государственный педагогический университет»
(ТГПУ)

УТВЕРЖДАЮ
Декан физико-математического факультета
_____
Е.Г. Пьяных, к.п.н., доцент

«26» мая 2016 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

ОСНОВЫ КРИПТОГРАФИИ

Направление подготовки: *44.03.05 Педагогическое образование (с двумя профилями подготовки)*

Направленности (профили): *Математика и Информатика*

Форма обучения: *очная*

1. Место учебной дисциплины (модуля) в структуре образовательной программы

Учебная дисциплина относится к вариативной части блока 1 и является дисциплиной по выбору обучающегося.

Дисциплины, предшествующие изучению данной дисциплины: «Теоретические основы прикладной математики и информатики».

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОП

Дисциплина обеспечивает формирование следующей компетенции:

✓ готовность использовать теоретические и практические знания в области науки и образования по направленности (профилю) образовательной программы (ПК-15).

3. Содержание учебной дисциплины (модуля)

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.

4. Трудоемкость дисциплины (модуля) по видам учебных занятий, самостоятельной работы обучающихся и формам контроля

4.1. Очная форма обучения

Объем в зачетных единицах: 2.

4.1.1. Виды учебных занятий, самостоятельная работа обучающихся, формы контроля (в академических часах)

Вид учебной работы	Всего часов	Распределение по семестрам (в академических часах)
		10

Лекции	10	10
Лабораторные работы	10	10
Практические занятия (семинары)	20	20
Самостоятельная работа	32	32
Курсовая работа		
Другие виды занятий		
Формы текущего контроля		тест
Формы промежуточной аттестации		зачёт
Итого часов	72	72

4.1.2. Содержание учебной дисциплины (модуля), структурированное по темам (разделам)

№п/п	Наименование темы (раздела) дисциплины	Всего часов	Аудиторные занятия (в часах)			Самостоятельная работа (в часах)
			Лекции	Практические занятия (семинары)	Лабораторные работы	
1	Кодирование информации.	14	2	2	4	6
2	Симметрические методы шифрования.	15	2	2	4	7
3	Несимметрические методы шифрования.	15	2	2	4	7
4	Электронная подпись.	14	2	2	4	6
5	Защита данных в информационных системах.	14	2	2	4	6
	Итого:	**72**	**10**	**10**	**20**	**32**

4.1.3. Лабораторный практикум

№ п/п	Наименование темы (раздела) дисциплины	Наименование лабораторных работ
1.	Кодирование информации.	Различные методы кодирования и декодирования информации
2.	Симметрические методы шифрования.	Код Цезаря, методы подстановок и перестановок, метод «исключающего или»
3.	Несимметрические методы шифрования.	Метод Эйлера. Метод RSA
4.	Электронная подпись.	Использование метода RSA для электронной подписи.
5.	Защита данных в информационных системах.	Использование хеш-значений при авторизации

5. Перечень учебно-методического обеспечения по дисциплине (модулю)

5.1. Основная учебная литература:

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

5.2. 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.

5.3. Перечень ресурсов информационно-коммуникационной сети Интернет, необходимых для освоения дисциплины (модуля)

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

В качестве примеров ссылок на интернет-источники можно привести:

http://intuit.ru

http://lib.ru

5.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

№ п/п	Номера разделов (тем) 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.

6. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Для проведения занятий необходимы: лекционная аудитория, кабинет информатики и методики обучения информатике.

7. Методические указания для обучающихся по освоению дисциплины (модуля)

Обучающимся 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 обучающимся при обсуждении;

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

8. Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю)

Представлен в виде отдельного документа (приложение к рабочей программе учебной дисциплины (модуля).

Рабочая программа учебной дисциплины (модуля) составлена в соответствии с учебным планом, федеральным государственным образовательным стандартом высшего образования по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки).

Рабочая программа учебной дисциплины (модуля) составлена Стасем А.Н., к.т.н., заведующим кафедрой информатики.

Рабочая программа учебной дисциплины (модуля) утверждена на заседании кафедры информатики

Протокол №10 от «26» мая 2016 года

Зав. кафедрой информатики _____ А.Н. Стась, к.т.н.

Рабочая программа учебной дисциплины (модуля) одобрена методической комиссией физико-математического факультета

Протокол № 9 от « 26 » мая 2016 года

Председатель учебно-методической комиссии физико-математического факультета _____ З.А. Скрипко, д.п.н, профессор