МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «ИНГУШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФИЗИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

АННОТАЦИЯ

рабочей программы учебной дисциплины

Б1.В.ДВ.05.02 ОСНОВЫ КРИПТОГРАФИИ

Направление подготовки *бакалавриата*

09.03.02 «Информационные системы и технологии»

1. Цель изучения дисциплины

Цель дисциплины – сформировать компетенции обучающегося в области математического аппарат криптозащиты и криптоанализа, современных криптографических протоколов, практическог использования криптографических средств защиты информации.

Задачами преподавания дисциплины являются:

– Рассмотреть наиболее распространённые криптографические протоколы, а также основны методы криптоанализа.;

– Раскрыть принципы математических и вычислительных моделей криптографически процессов, их оптимизация и выработка направлений совершенствования;

– Показать особенности различных криптографических протоколов и возможностей и применения.

2. Место дисциплины в структуре ОПОП ВО бакалавриата

Дисциплина «Основы криптографии» относится к базовой части Б1. Освоение дисциплины **основывается** на знаниях студентов, полученных ими в ходе изучения дисциплин предыдущих курсов: **«Интеллектуальные информационные системы и технологии», «Архитектура информационных систем», «Теория информационных процессов и систем».** Данная дисциплина необходима **для освоения** следующих дисциплин: **«Инструментальные средства информационных систем», «Методы и средства проектирования информационных систем и технологий».**

3. Результаты освоения дисциплины (модуля) Б1.В.ДВ.05.02 «Основы криптографии»

Код и наименование компетенции	Индикаторы	Дескрипторы
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1.: понимает виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность. УК-2.2.: проводит анализ поставленной цели и формулировать задачи, которые необходимо решить	**Знать**: виды ресурсов ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность. **Уметь:** проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно правовую документацию в сфере профессиональной

		для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности.	деятельности.
	Профессиональные компетенции (ПК)		
	ПК-4. Способность выполнять работы по обеспечению функционирования баз данных и обеспечению их информационной безопасности	ПК-4.1: использует специальные знания по работе с установленной БД; общие основы решения практических задач по восстановлению БД и проверке корректности восстановленных данных; основы управления учетными записями пользователей; ПК-4.2: выполняет регламентные процедуры по резервированию данных; выбирать способ действия из известных; контролировать оценивать и корректировать свои действия; выполнять регламентные процедуры по восстановлению и проверке корректности восстановленных данных; выбирать способ действия из известных; контролировать оценивать и корректировать свои действия; применять специальные процедуры управления правами доступа пользователей ПК-4.3: запускает процедуры резервного копирования; мониторинга выполнения процедуры резервного копирования; контроля завершения процедуры резервного копирования; запуска процедуры восстановления БД; мониторинга выполнения	**Знать:** специальные знания по работе с установленной БД; общие основы решении практических задач по восстановлению БД и проверке корректности восстановлены данных; специальные знаний по работе с установленной БД основы управления учетными записями пользователей; специальные знания по работам с установленной БД. **Уметь:** выполнять регламентные процедуры п резервированию данных; выбирать способ действия и известных; контролировать оценивать и корректировать свои действия; выполнят , регламентные процедуры п восстановлению и проверки корректности восстановлены данных; выбирать способ действия из известных контролировать, оценивать корректировать свои действия применять специальные процедуры управления правами доступа пользователей; **Владеть навыками:** запуск процедуры резервного копирования; мониторинг выполнения процедуры резервного копирования; контроля завершения ; процедуры резервного копирования; запуска процедуры восстановления БД мониторинга выполнения процедуры восстановления БД контроля завершения процедуры восстановления БД назначения прав доступа пользователей к БД; изменений прав доступа пользователей к БД

		процедуры восстановления БД; контроля завершения процедуры восстановления БД; назначения прав доступа пользователей к БД изменения прав доступа пользователей к БД; контроля соблюдения прав доступа пользователей к БД.	
	Профессиональные компетенции (ПК)		
	ПК-8. Способность выполнять работы по разработке компонентов системных программных продуктов: компилятор, загрузчиков, сборщиков, системных утилит, драйверов устройств, по созданию инструментальных средств программирования	ПК-8.1.: понимает синтаксис выбранного языка программирования, особенности программирования на этом языке, стандартные библиотеки языка программирования; методологии разработки программного обеспечения; методологии и технологии проектирования и использования баз данных; технологии программирования; особенности выбранной среды программирования и системы управления базами данных; компоненты программно-технических архитектур, существующие приложения и интерфейсы взаимодействия с ними; ПК-8.2: применяет выбранные языки программирования для написания программного кода; использовать выбранную среду программирования и средства системы управления базами данных; использовать возможности имеющейся технической и/или программной архитектуры;	**Знать:** синтаксис выбранного языка программирования, особенности программирования на этом языке, стандартные библиотеки языка программирования; методологии разработки программного обеспечения; методологии и технологии проектирования и использования баз данных; технологии программирования; особенности выбранной среды программирования и системы управления базами данных; компоненты программно-технических архитектур, существующие приложения и интерфейсы взаимодействия с ними; Уметь: применять выбранные языки программирования для написания программного кода; использовать выбранную среду программирования и средства системы управления базами данных; использовать возможности имеющейся технической и/или программной архитектуры
4.	**Структура и содержание дисциплины**		

4.1. Структура дисциплины

Вид учебной работы	Всего	Порядковый номер семестра			
		5			
Общая трудоемкость дисциплины всего (в з.е.), в том числе:	5				
Курсовой проект (работа)	-				
Аудиторные занятия всего (в акад. часах), в том числе:	68				
Лекции	36				
Практические занятия, семинары	-	-			
Лабораторные работы	32				
Самостоятельная работа всего (в акад. часах), в том числе:	85				
КСР	-	-			
Экзамен	27	-	27		
Общая трудоемкость дисциплины	180ч.				

4.2. Содержание дисциплины

Тема 1. Введение в криптографию. Основные понятия и определения.
Тема 2. Математические основы криптографии
Тема 3. Стойкость криптоалгоритмов
Тема 4. Поточные шифры
Тема 5. Блочные шифры
Тема 6. Криптографические протоколы
Тема 7. Построение криптографических примитивов
Тема 8. Симметричные криптосистемы
Тема 9. Алгоритм DES
Тема 10. Алгоритм ГОСТ 28147 -89
Тема 11. Ассиметричные криптосистемы
Тема 12. Алгоритм RSA
Тема 13. Электронная цифровая подпись
Тема 14. Основные криптоаналитические методы
Тема 15. Дискретное логарифмирование
Тема 16. Факторизация целых чисел (Поллард)
Тема 17. Псевдослучайные последовательности. Линейные рекуррентные последовательности как псевдослучайные последовательности

5. Образовательные технологии

	При осуществлении образовательного процесса по дисциплине используются следующие информационные технологии: 1. Internet - технологии: WWW(англ.WorldWideWeb- Всемирная Паутина) - технология работы в сети с гипертекстами; FTP(англ. FileTransferProtocol- протокол передачи файлов) - технология передачи по сети файлов произвольного формата; IRC(англ.InternetRelayChat- поочередный разговор в сети, чат) - технология ведения переговоров в реальном масштабе времени, дающая возможность разговаривать с другими людьми по сети в режиме прямого диалога; ICQ(англ.Iseekyou- я ищу тебя, можно записать тремя указанными буквами) - технология ведения переговоров один на один в синхронном режиме. 2. Дистанционное обучение с использованием ЭИОС на платформе Moodle. 3. Технология мультимедиа в режиме диалога. 4. Технология неконтактного информационного взаимодействия (виртуальные кабинеты, лаборатории). 5. Гипертекстовая технология (электронные учебники, справочники, словари, энциклопедии) и т.д.
6.	**Используемые ресурсы информационно-телекоммуникационной сети «Internet»; информационные технологии, программные средства и информационно-справочные системы**
	1.Электронная информационно-образовательная среда АНО ВО "СЗТУ" (ЭИОС СЗТУ) [Электронный ресурс]. - Режим доступа: http://edu.nwotu.ru/ 2.Учебно-информационный центр АНО ВО "СЗТУ" [Электронный ресурс]. - Режим доступа: http://lib.nwotu.ru:8087/jirbis2/ 3.Электронно-библиотечная система IPRbooks [Электронный ресурс]. - Режим доступа: http://www.iprbookshop.ru/ 4.Информационная система "Единое окно доступа к образовательным ресурсам" [Электронный ресурс]. - Режим доступа: http://window.edu.ru/ 5.Информационная системы доступа к электронным каталогам библиотек сферы образования и науки (ИС ЭКБСОН) [Электронный ресурс]. - Режим доступа: http://www.vlibrary.ru/ **Программное обеспечение** При осуществлении образовательного процесса по дисциплине используются следующие информационные технологии: Internet- технологии: WWW(англ.WorldWideWeb- Всемирная Паутина) - технология работы в сети с гипертекстами; FTP(англ. FileTransferProtocol- протокол передачи файлов) - технология передачи по сети файлов произвольного формата; IRC(англ.InternetRelayChat- поочередный разговор в сети, чат) - технология ведения переговоров в реальном масштабе времени, дающая возможность разговаривать с другими людьми по сети в режиме прямого диалога; ICQ(англ.Iseekyou- я ищу тебя, можно записать тремя указанными буквами) - технология ведения переговоров один на один в синхронном режиме. Дистанционное обучение с использованием ЭИОС на платформе Moodle. Технология мультимедиа в режиме диалога. Технология неконтактного информационного взаимодействия (виртуальные кабинеты, лаборатории). Гипертекстовая технология (электронные учебники, справочники, словари, энциклопедии) и т.д.

	Программное обеспечение: ППП MSOffice2010
7.	**Формы текущего контроля**
	• Коллоквиум; • Тест; • Контрольная работа; • Отчеты студентов по лабораторным работам.
8.	**Форма промежуточного контроля**
	Экзамен

Разработчик: старший преподаватель кафедры «Информационные системы и технологии» Цуроев И.М.