

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новгородский государственный университет имени Ярослава Мудрого»
Институт информационных и электронных систем
Кафедра прикладной математики и информатики



УТВЕРЖДАЮ
Директор ИЭИС

С.И. Эминов
2017г.

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Учебный модуль по направлению подготовки
01.03.02 – прикладная математика и информатика

Рабочая программа

СОГЛАСОВАНО

Разработал

начальник учебного отдела
О.Б. Широколобова

Доцент кафедры ПМИ НовГУ
Т.В. Жгун
«10» февраля 2017 г.

«27» 03 2017

Принято на заседании кафедры КПМИ

1 Цели и задачи учебного модуля

Целью учебного модуля (УМ) является формирование компетентности студентов в области защиты информации, способствующей становлению их готовности к решению задач профессиональной деятельности; раскрытие сущности и значения информационной безопасности и защиты информации, определение методологических и технических основ различных аспектов защиты информации и связи между ними.

Основными задачами УМ являются:

- определение базовых понятий информационной безопасности и защиты информации;
- определение угроз, каналов и способов несанкционированного доступа к информации;
- изучение основных методов и систем криптографической защиты информации; изучение основных типов политик безопасности и систем разграничения доступа;
- рассмотрение особенностей защиты информации в сетях;
- обзор нормативной базы в области защиты информации.
- формирование понимания студентами значимости знаний и умений в области защиты информации в процессе профессиональной деятельности;
- формирование системы знаний о методах защиты информации, позволяющей в будущем выстраивать на научной основе процессы профессиональной деятельности;
- подготовка студентов к профессиональной деятельности, связанной с выполнением проектов на основе современных вычислительных технологий.

Ведущие идеи учебного модуля:

- понимание особенностей применения методов защиты информации является важнейшей частью компетентности специалиста в сфере профессиональной деятельности;
- эффективные решения в профессиональной сфере в первую очередь основываются на анализе значения и возможных последствиях адекватного применения методов защиты информации.

2 Место учебного модуля в структуре ООП направления подготовки

Учебный модуль относится к базовой части блока Б1, читается в 8 семестре.

Для изучения необходимы знания и умения, полученные при изучении модулей «Линейная алгебра и аналитическая геометрия», «Математический анализ», «Теория вероятностей и математическая статистика», «Информатика» и «Алгоритмические языки», «Дискретная математика».

Знания и умения, полученные при изучении данного модуля, используются при прохождении производственной практики и при подготовке выпускной квалификационной работы.

3 Требования к результатам освоения учебного модуля

Процесс изучения УМ направлен на формирование компетенций:

- способность приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии (ОПК-2);
- способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4);
- способностью осуществлять целенаправленный поиск информации о новейших научных и технологических достижениях в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") и в других источниках (ПК-5).

В результате освоения УМ студент должен знать, уметь и владеть:

Код компетенции	Уровень освоения компетенции	Знать	Уметь	Владеть
ОПК-2	базовый	основные современные образовательные и информационные технологии, их достоинства и недостатки по сравнению с традиционными технологиями; сущность и значение информации в развитии современного информационного общества; основные понятия информационной безопасности и ее составляющих; опасности и угрозы в области информационной безопасности, в том числе в области информационной безопасности России	обмениваться научно-технической информацией, используя современные образовательные и информационные технологии, находить, классифицировать и использовать информационные интернет-технологии, базы данных, <i>web</i> -ресурсы, специализированное программное обеспечение для получения новых научных и профессиональных знаний; Применять основные требования к обеспечению информационной безопасности; Применять современные средства и методы защиты информационной безопасности.	навыками решения задач поиска и анализа научно-технической информации; Основными требованиями к обеспечению информационной безопасности; Современными средствами и методами защиты информационной безопасности.

Код компетенции	Уровень освоения компетенции	Знать	Уметь	Владеть
ОПК-4	базовый	Базовые понятия по защите информации на рабочем месте, в корпоративных сетях при входе в глобальные сети при решении стандартных задач профессиональной деятельности: криптоалгоритмы, используемые в современных стандартах шифрования данных; методы выбора криптографических параметров, обеспечивающих необходимую стойкость криптосистем; ключевые системы современных криптосистем и протоколы распределения ключей; перспективные направления криптографии; приложения криптографии к решению различных проблем защиты информации в компьютерных системах.	Применять базовые знания по защите информации на рабочем месте, в корпоративных сетях при входе в глобальные сети при решении стандартных задач профессиональной деятельности: криптоалгоритмы, используемые в современных стандартах шифрования данных; методы выбора криптографических параметров, обеспечивающих необходимую стойкость криптосистем; ключевые системы современных криптосистем и протоколы распределения ключей; перспективные направления криптографии; приложения криптографии к решению различных проблем защиты информации в компьютерных системах —	базовыми знаниями по защите информации на рабочем месте, в корпоративных сетях при входе в глобальные сети при решении стандартных задач профессиональной деятельности: криптоалгоритмы, используемые в современных стандартах шифрования данных; методы выбора криптографических параметров, обеспечивающих необходимую стойкость криптосистем; ключевые системы современных криптосистем и протоколы распределения ключей; перспективные направления криптографии; приложения криптографии к решению различных проблем защиты информации в компьютерных системах

Код компетенции	Уровень освоения компетенции	Знать	Уметь	Владеть
ПК-5	Базовый	- структуру и основные методы индексации, поиска, сортировки и отбора информации;	– строить эффективные поисковые фразы в большинстве популярных поисковых машин Интернет; .	навыками работы с поисковыми машинами в сети Интернет; - средствами поиска в профессиональных электронных библиотеках.

4 Структура и содержание учебного модуля

4.1 Трудоемкость учебного модуля

Учебная работа (УР)	Всего	Распределение по семестрам		Коды формируемых компетенций
			8 сем	
Трудоемкость модуля в зачетных единицах (ЗЕ)	5		5	
Распределение трудоемкости по видам УР в академических часах (АЧ):	180		180	ОПК2, ОПК4 ПК5
- лекции	20		20	
-практические занятия	25		25	
-лабораторные работы	25		25	
- аудиторная СРС	23		23	
- внеаудиторная СРС в том числе курсовая работа	110		110	
Аттестация: экзамен	36		36	

4.2 Содержание и структура разделов учебного модуля

1. **Введение.** Роль информации в современном обществе. Проблемы информации вообще и управления как информационный процесс. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности; классификация атак; модели сетевой безопасности и безопасности информационной системы.
2. **Традиционное шифрование:** классические методы. Основные понятия и определения. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера, Вернама. Дисковые шифраторы. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернама.
3. **Алгоритмы симметричного шифрования.** Основные понятия, относящиеся к алгоритмам симметричного шифрования: ключ шифрования, plaintext, ciphertext. Определение стойкости алгоритма, типы операций, используемые в алгоритмах симметричного шифрования. Сеть Фейштеля. Основные понятия криптоанализа, линейный и дифференциальный криптоанализ. Описание алгоритмов DES и тройного DES. Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147, а также режимы их выполнения. Различные способы создания псевдослучайных чисел

4. **Асимметричные системы шифрования** (системы с открытым ключом). Понятия однонаправленной функции и однонаправленной функции с лазейкой. Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана, схема Эль-Гамала. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости
5. **Хэш-функции и аутентификация сообщений.** Основные понятия, относящиеся к обеспечению целостности сообщений с помощью MAC и хэш-функций; представлены простые хэш-функции и сильная хэш-функция MD5. Сильные хэш-функции SHA-1, SHA-2 и ГОСТ 3411. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC.
6. **Цифровая подпись.** Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись, стандарты цифровой подписи ГОСТ 3410 и DSS.
7. **Криптография с использованием эллиптических кривых.** Математические понятия, связанные с эллиптическими кривыми, в частности задача дискретного логарифмирования на эллиптической кривой. Аналог алгоритма Диффи - Хеллмана на эллиптических кривых, алгоритма цифровой подписи на эллиптических кривых и алгоритма шифрования с открытым ключом получателя на эллиптических кривых.
8. **Безопасность современных сетевых технологий.** Способы несанкционированного доступа к информации в компьютерных сетях. Классификация способов несанкционированного доступа и жизненный цикл атак. Способы противодействия несанкционированному межсетевому доступу. Функции меж сетевого экранирования. Построение защищенных виртуальных сетей. Способы создания защищенных виртуальных каналов. Обзор протоколов. Безопасность в открытых сетях. Инфраструктура на основе криптографии с открытыми ключами (ИОК). Цифровые сертификаты. Управление цифровыми сертификатами. Управление ключами.
9. **Методы и средства встраивания скрытой служебной информации для управления правами доступа к информационным ресурсам.** Понятие стеганографии. Задача встраивания скрытой служебной информации (цифровых водяных знаков) в аудио и видеосигналы. Основные методы и алгоритмы встраивания и обнаружения водяных знаков. Встраивание водяных знаков и сжатие информации. Виды атак на информационные ресурсы, содержащие водяные знаки.

4.3 Тематика практических занятий

№ раздела УМ	Наименование	Трудоемкость, ак.час
1.2	Традиционное шифрование	6
1.3	Алгоритмы симметричного шифрования	6
1.4	Системы с открытым ключом	5
1.5, 1.6	Аутентификация сообщений. Цифровая подпись	5
1.8	Сетевая безопасность	3

4.4 Лабораторный практикум

№ раздела УМ	Наименование лабораторных работ	Трудоемкость, ак.час
1.2	Традиционное шифрование	5
1.3	Алгоритмы симметричного шифрования. VS-AES	5
1,4	Математические основы криптографии	5
1,4	Системы с открытым ключом	5
1.5, 1.6	Аутентификация сообщений. Цифровая подпись	5

4.5 Организация изучения учебного модуля

Методические рекомендации по организации изучения УМ с учетом использования в учебном процессе активных и интерактивных форм проведения учебных занятий даются в Приложении А.

5 Контроль и оценка качества освоения учебного модуля

Контроль качества освоения студентами УМ и его составляющих осуществляется непрерывно в течение всего периода обучения с использованием балльно-рейтинговой системы (БРС), являющейся обязательной к использованию всеми структурными подразделениями университета.

Для оценки качества освоения модуля используются формы контроля: текущий – регулярно в течение всего семестра, рубежный и семестровый (экзамен) – по окончании изучения УМ.

Рубежный контроль проходит на 18 неделе, по окончании изучения УМ и осуществляется посредством экзамена и подсчетом суммарных баллов за весь период изучения УМ. Пороговому уровню соответствует 125 баллов, максимальное количество баллов за рубежный контроль – 250 баллов. Максимальное количество баллов, получаемое на экзамене, – 50. Максимальное количество баллов, полученных при изучении УМ – 300 баллов.

Оценка качества освоения модуля осуществляется с использованием фонда оценочных средств, разработанного для данного модуля, по всем формам контроля в соответствии с положением от 27.09.2011 № 32 «Об организации учебного процесса по основным образовательным программам высшего профессионального образования».

Оценка качества освоения модуля осуществляется с использованием фонда оценочных средств, разработанного для данного модуля.

Содержание видов контроля и их график отражены в технологической карте учебного модуля (Приложение Б). Паспорта компетенций представлены в приложении В.

6 Учебно-методическое и информационное обеспечение

Учебно-методическое и информационное обеспечение учебного модуля представлено Картой учебно-методического обеспечения (Приложение Г).

7 Материально-техническое обеспечение учебного модуля

Освоение дисциплины «Методы защиты информации» предполагает использование следующего материально-технического обеспечения: мультимедийный проектор, презентации по курсу, компьютерный класс, представляющий собой рабочее место преподавателя и не менее 10 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети НовГУ и находятся в едином домене.

Программное обеспечение:

1. Математическая система *MathCAD 13.0 (MathSoft)* или Профессиональная среда для выполнения вычислений *Maple (Waterloo Maple Software)*.
2. Электронные таблицы *Excel*.
3. Системы программирования: *Turbo Pascal, Borland C++*.

Приложения (обязательные):

А – Методические рекомендации по организации изучения учебного модуля

Б – Технологическая карта

В – Паспорта компетенций

Г – Карта учебно-методического обеспечения УМ

Приложение А

Методические рекомендации по организации изучения учебного модуля «Методы защиты информации»

Учебный модуль «Методы защиты информации» состоит из взаимосвязанных разделов, по которым предусмотрены лекционные, практические и лабораторные занятия. В таблице А.1 отражены разделы модуля, технологии и формы проведения занятий, задания по самостоятельной работе студента и ссылки на необходимую литературу. Содержание разделов представлено в п. 4.2 рабочей программы модуля.

А.1 Методические рекомендации по теоретической части учебного модуля

Теоретическая часть модуля направлена на формирование системы знаний о сфере применения основных понятий информационной безопасности и методах защиты информации. Основное содержание теоретической части излагается преподавателем на лекционных занятиях, а также усваивается студентом при знакомстве с дополнительной литературой, которая предназначена для более глубокого овладения знаниями основных дидактических единиц соответствующего раздела и указана в таблице А.1.

В начале лекции проводится, опрос или собеседование (не более 20 мин.) для экспресс-оценки уровня усвоения теоретического материала.

А.2 Методические рекомендации по практическим занятиям

Цель практических занятий – формирование у студентов умения работать в коллективе, способности к кооперации с коллегами, способности находить профессиональные решения и компетентности студентов в области научной и научно-исследовательской деятельности, способствующей становлению их готовности приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии, критически переосмысливать накопленный опыт и изменять при необходимости вид и характер своей профессиональной деятельности, а также умение применить теоретические сведения к решению конкретных задач.

Практические занятия в большинстве своем строятся следующим образом:

- 20% аудиторного времени отводится на объяснение решения типовой задачи у доски или на объяснение задания;
- 70% аудиторного времени – самостоятельное решение задач студентами или их коллективное выполнение упражнений;
- 10% аудиторного времени в конце текущего занятия – разбор типовых ошибок при решении задач или подведение итогов выполнения упражнений.

Форма проведения лекционных и практических занятий указана в таблице А.1.

Таблица А.1 - Организация изучения учебного модуля «Методы защиты информации»

Раздел модуля	Технология и форма проведения лекционных и практических занятий	Задания на СРС	Дополнительная литература и интернет-ресурсы
Введение.. Основные понятия информационной безопасности	вводная лекция информационная лекция, лекция – демонстрация собеседование	подготовиться к собеседованию (внеауд. СРС); – собеседование (ауд. СРС)	Конеев И. Р. Информационная безопасность предприятия / Искандер Корнеев, Андрей Беляев. - СПб. : БХВ-Петербург, 2003. - 733 с. Ф2-3(13)
Традиционное шифрование	информационная лекция; лекция – демонстрация решение задач ПЗ №5 выполнение ЛР№1; собеседование (защита ЛР№1)	подготовиться к собеседованию (внеауд. СРС); – собеседование (ауд. СРС) – выполнение ДЗ1	Мао Венбо. Современная криптография. Теория и практика = Modern cryptography / Пер. с англ. и ред. Д.А. Ключина. - М. : Вильямс, 2005. - 763с. Ф1-3 Танова Э.В. Введение в криптографию: как защитить свое письмо от любопытных : учеб. пособие. - М. : БИНОМ. Лаборатория знаний, 2007, 2008. – 79 с.
Алгоритмы симметричного шифрования	информационная лекция; решение задач ПЗ №5 выполнение ЛР№ 2; собеседование (защита ЛР№ 2,)	подготовиться к собеседованию (внеауд. СРС); выполнение ДЗ1 – собеседование (ауд. СРС)	Рябко Б.Я. Криптографические методы защиты информации : учеб. пособие для вузов. - М. : Горячая линия-Телеком, 2005. - 229с. Ф1-3 Рябко Б.Я. Основы современной криптографии для специалистов в информационных технологиях / РАН, Ин-т вычисл. технологий; Сиб. гос. ун-т телекоммуникаций и информатики. - М. : Научный мир, 2004. - 172с. – Ф1-4
Асимметричные системы шифрования.	информационная лекция; решение задач ПЗ №5 выполнение ЛР№ 3; 4 собеседование (защита ЛР№ 3, 4)	подготовиться к собеседованию (внеауд. СРС); – собеседование (ауд. СРС) выполнение ДЗ2	Рябко Б.Я. Криптографические методы защиты информации : учеб. пособие для вузов. - М. : Горячая линия-Телеком, 2005. - 229с. Ф1-3 Рябко Б.Я. Основы современной криптографии для специалистов в информационных технологиях / РАН, Ин-т вычисл. технологий; Сиб. гос. ун-т телекоммуникаций и информатики. - М. : Научный мир, 2004. - 172с. – Ф1-4 Молдовян Н.А. Введение в криптосистемы с открытым ключом : Учеб. пособие. - СПб. : БХВ-Петербург, 2005. - 286с.-(Ф1-5 Молдовян Н.А. Практикум по криптосистемам с открытым

Раздел модуля	Технология и форма проведения лекционных и практических занятий	Задания на СРС	Дополнительная литература и интернет-ресурсы
			ключом. - СПб. : БХВ-Петербург, 2007. - 298с. Скляров И.С. Головоломки для хакера. - СПб. : БХВ-Петербург, 2005. - 319с. Ф1-3 Полянская О.Ю. Инфраструктуры открытых ключей : учеб. пособие. - М. : Интернет-Университет Информ. Технологий : БИНОМ. Лаборатория знаний, 2007. - 367с. Ф1-5
аутентификация сообщений	информационная лекция; решение задач ПЗ №5 выполнение ЛР№ 4;5 собеседование (защита ЛР№4)	подготовиться к собеседованию (внеауд. СРС); выполнение ДЗ1 – собеседование (ауд. СРС)	Зубов А.Ю. Математика кодов аутентификации. - М. : Гелиос АРВ, 2007. - 479, Ф1-2 Полянская О.Ю. Инфраструктуры открытых ключей : учеб. пособие. - М. : Интернет-Университет Информ. Технологий : БИНОМ. Лаборатория знаний, 2007. - 367с. Ф1-5 Рябко Б.Я. Криптографические методы защиты информации : учеб. пособие для вузов. - М. : Горячая линия-Телеком, 2005. - 229с. Ф1-3 Рябко Б.Я. Основы современной криптографии для специалистов в информационных технологиях / РАН,Ин-т вычисл.технологий;Сиб.гос.ун-т телекоммуникаций и информатики. - М. : Научный мир, 2004. - 172с. – Ф1-4
Криптография с использованием эллиптических кривых	информационная лекция; решение задач ПЗ №5	подготовиться к практическому занятию (внеауд. и ауд. СРС))	Болотов А.А. Элементарное введение в эллиптическую криптографию:Протоколы криптографии на эллиптических кривых. - М. : КомКнига, 2006. - 274с. : ил. - Библиогр.:с.264-268. - Прил.:с.196-263 Ф1-1
Сетевая безопасность	информационная лекция; решение задач ПЗ	подготовиться к практическому занятию (внеауд. и ауд. СРС))	Конахович Г.Ф. Компьютерная стеганография : Теория и практика. - Киев : МК-Пресс, 2006. - 283с. Ф1-2

Приложение Б

Технологическая карта УМ «Методы защиты информации»
семестр 8, ЗЕТ 5, вид аттестации экзамен
Акад. часов 180 , баллов рейтинга 250

№ и наименование раздела учебного модуля, КП/КР	№ неде-ли сем.	Трудоемкость, ак.час					Форма текущего контроля успеваемости (в соотв. с паспортом ФОС)	Максим. кол-во баллов рейтинга
		Аудиторные занятия				С Р С		
		ЛЕК	ПЗ	ЛР	А СРС			
Тема 1. Введение	1-2	2	3		4	4	-	
Тема 2. Традиционное шифрование: классические методы	3-4	4	6	6	4	10	ЛР ДЗ1	24 40
Тема 3. Алгоритмы симметричного шифрования	5-8	4	6	6	4	10	ЛР	24
Тема 4. Асимметричные системы шифрования	9-10	2	4	7		10	ЛР ДЗ2	24 40
Тема 5. Хэш-функции и аутентификация сообщений	11-12	2	2		4	10	- ЛР-	24
Тема 6. Цифровая подпись	13-14	2	2	6	4	10	- ЛР	24
Тема 7. Криптография с использованием эллиптических кривых	15-16	2	2		3	10		
Тема 8. Безопасность современных сетевых технологий	17-18	2	2			10		
Рубежный контроль		Рубежный контроль – не менее 125 баллов из 250						
Семестровый контроль Экзамен						36	Э	50
Итого:		20	25	25	23	110		250

Приложение В

Паспорта компетенций ОПК2, ОПК4, ПК5
способность приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии (ОПК-2)

Уровни	Показатели	Оценочная шкала		
		удовлетворительно	хорошо	отлично
Базовый уровень	Применяет цифровые технологии для сбора, оценки и использования информации в области защиты информации	Понимает и использует информационные технологии и системы для получения знаний в области защиты информации	Выбирает и использует информационные технологии и системы для получения знаний в области защиты информации	переносит полученные знания в новые сферы в области защиты информации
	Приобретет новые научные и профессиональные знания	Демонстрирует знание основ методов защиты информации Испытывает трудности при демонстрации знаний о методах защиты информации Недостаточно точно реализует относящиеся к дисциплине методики и технологии	Недостаточно логично излагает полученные знания в области методов защиты информации Недостаточно точно реализует относящиеся к дисциплине методики и технологии	Ясно и логично излагает полученные знания в области защиты информации Точно реализует относящиеся к дисциплине методики и технологии Демонстрирует понимание качества исследований, выполненных средствами методов защиты информации

способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4)

Уровни	Показатели	Оценочная шкала		
		удовлетворительно	хорошо	отлично
Базовый уровень	Понимает сущность и значение информации в развитии современного информационного общества	Толкует информацию как важный фактор расширения эрудиции и профессионального саморазвития • Рассказывает о влиянии информации на развитие современного общества • Избирает информацию, необходимую для своей жизнедеятельности и профессиональной деятельности	Высказывает суждение о роли информации в совершенствовании содержания воспитательно-образовательной работы • Дает оценку информации с точки зрения ее значимости и пользы для развития современного общества □	Разрабатывает на основе полученной информации методологию исследовательского поиска и технологию реализации творческой идеи, проекта
	Сознаёт опасности и угрозы, возникающие в этом процессе	Перечисляет возможные опасности и угрозы информационной безопасности • Объясняет причины возникновения опасностей и угроз • Демонстрирует средства и методы защиты от опасностей и угроз	Классифицирует угрозы по степени опасности • Анализирует возможные последствия опасностей и угроз	Организует защиту от возможных информационных опасностей и угроз
	Соблюдает основные требования информационной безопасности	Знает основные требования информационной безопасности • Понимает значение государственной тайны и информационной безопасности • Применяет на практике механизмы соблюдения информационной безопасности □	Анализирует источники информационной опасности • Оценивает последствия нарушения информационной безопасности	Разрабатывает методы обеспечения информационной безопасности • Организует контроль защиты информационной безопасности

способность осуществлять целенаправленный поиск информации о новейших научных и технологических достижениях в информационно-телекоммуникационной сети "Интернет" и в других источниках (ПК-5)

Уровни	Показатели	Оценочная шкала		
		удовлетворительно	хорошо	отлично
Базовый уровень	Знание - основные методы индексации, поиска, сортировки и отбора информации;	Имеет общее представление о теоретических и методологических основах базовых и некоторых специальных разделов индексации, поиска, сортировки и отбора информации, классификаторов ; но не может предложить способы их использования при решении конкретных задач	Имеет общее представление о теоретических и методологических основах базовых и некоторых специальных разделов индексации, поиска, сортировки и отбора информации, может предложить отдельные примеры их использования при решении задач профессиональной деятельности	Имеет четкое представление о теоретических и методологических основах базовых и некоторых специальных разделов индексации, поиска, сортировки и отбора информации, в, может предложить примеры их использования при решении задач профессиональной деятельности
	Умение – строить эффективные поисковые фразы в большинстве популярных поисковых машин Интернет;	Испытывает трудности в построении эффективных поисковых фраз,	Не всегда корректно использует основные методы построения эффективных поисковых фраз,;	Способен правильно использовать основные методы построения эффективных поисковых фраз, применении
	Владение - навыками работы с поисковыми машинами в сети Интернет; - средствами поиска в профессиональных электронных библиотеках;	Испытывает трудности при использовании навыков работы с поисковыми машинами в сети Интернет; - средствами поиска в профессиональных электронных библиотеках;	Недостаточно уверенно использует Навыки работы с поисковыми машинами в сети Интернет; - средствами поиска в профессиональных электронных библиотеках;	Полностью владеет методами работы с поисковыми машинами в сети Интернет; - средствами поиска в профессиональных электронных библиотеках;

Приложение Г

Карта учебно-методического обеспечения

Учебного модуля «Методы защиты информации »

Направление 01.03.02 Прикладная математика и информатика

Формы обучения очная Курс 4 Семестр 8

Часов: всего 180 , лекций 20, практ. зан. 25, лаб. раб. 25 , СРС 110

Обеспечивающая кафедра Прикладная математика и информатика

Таблица 1- Обеспечение учебного модуля учебными изданиями

Библиографическое описание* издания (автор, наименование, вид, место и год издания, кол. стр.)	Кол. экз. в библ. НовГУ	Наличие в ЭБС
Учебники и учебные пособия		
1 Мельников В. П. Защита информации : учебник : для бакалавров / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М. : Академия, 2014. - 295, [2] с. : ил. - (Высшее образование, Информационная безопасность) (Бакалавриат). Ф1-4	5	
2.Лапони́на О.Р. Основы сетевой безопасности:криптографические алгоритмы и протоколы взаимодействия:Курс лекций:Учеб.пособие/Под ред.В.А.Сухомлина.-М.:Интернет-Ун-т Информ.Технологий,2005.-604 Ф1-2	2	есть электр. вариант
Учебно-методические издания		
1 Рабочая программа модуля с приложениями «Методы защиты информации/Авт.-сост. Т.В. Жгун ; НовГУ. – В.Новгород, 2016. – 20 с.		
Жгун Т.В. Методы защиты информации.. [Электронный ресурс]: конспект лекций. – Великий Новгород, 2014. – 171 с. – Режим доступа: https://novsu.bibliotech.ru/Catalog/Index		
Жгун Т.В. Методы защиты информации. Методические указания к выполнения лабораторных работ. [Электронный ресурс] : методические указания . – Великий Новгород, 2013. – 40 с. – Режим доступа: https://novsu.bibliotech.ru/Catalog/Index	10	
Жгун Т.В. Методы защиты информации. Методические указания к практическим занятиям. [Электронный ресурс] : методические указания . – Великий Новгород, 2013. – 64 с. – Режим доступа: https://novsu.bibliotech.ru/Catalog/Index		

Таблица 2 – Информационное обеспечение учебного модуля

Название программного продукта, интернет-ресурса	Электронный адрес	Примечание
Антивирусная защита компьютерных систем - [Электронный ресурс] НОУ «ИНТУИТ», 2003 – 2016: Режим доступа: http://www.intuit.ru/studies/courses/2259/155/info /, свободный. - Загл. с экрана (дата обращения: 17.11.2016).	http://www.intuit.ru/studies/courses/2259/155/info	Курс Интернет-университета информационных технологий..
Безопасность сетей Антивирусная защита компьютерных систем - [Электронный ресурс] НОУ «ИНТУИТ», 2003 – 2016: Режим доступа: http://www.intuit.ru/studies/courses/102/102/info , свободный. - Загл. с экрана (дата обращения: 17.11.2016)..	http://www.intuit.ru/studies/courses/102/102/info	Курс Интернет-университета информационных технологий.
Введение в защиту информации от внутренних ИТ-угроз [Электронный ресурс] НОУ «ИНТУИТ», 2003 – 2016: Режим доступа: http://www.intuit.ru/studies/courses/1013/172/info/ , свободный. - Загл. с экрана (дата обращения: 17.11.2016).	http://www.intuit.ru/studies/courses/1013/172/info	Курс Интернет-университета информационных технологий.
Вирусы и средства борьбы с ними [Электронный ресурс] НОУ «ИНТУИТ», 2003 – 2016: Режим доступа: http://www.intuit.ru/studies/courses/1042/154/info/ , свободный. - Загл. с экрана (дата обращения: 17.11.2016).	http://www.intuit.ru/studies/courses/1042/154/info	Курс Интернет-университета информационных технологий Рассматриваются основы теории компьютерных вирусов, технологии борьбы с сетевыми угрозами, общие принципы комплексной системы антивирусной защиты корпоративной сети с использованием продуктов Лаборатории Касперского.
Криптографические основы безопасности [Электронный ресурс] НОУ «ИНТУИТ», 2003 – 2016: Режим доступа: http://www.intuit.ru/studies/courses/28/28/info/ , свободный. - Загл. с экрана (дата обращения: 17.11.2016).	http://www.intuit.ru/studies/courses/28/28/info	Курс Интернет-университета информационных технологий Курс Интернет-университета информационных технологий. Изучение методологических и алгоритмических основ и стандартов криптографической защиты информации..
Математика криптографии и теория шифрования безопасности [Электронный ресурс] НОУ «ИНТУИТ», 2003 – 2016: Режим доступа: http://www.intuit.ru/studies/courses/552/408/info/ , свободный. - Загл. с экрана (дата обращения: 17.11.2016).	http://www.intuit.ru/studies/courses/552/408/info	Курс Интернет-университета информационных технологий о криптографии с симметричными ключами и шифровании с помощью асимметричных ключей).

Основы информационной безопасности [Электронный ресурс] НОУ «ИНТУИТ», 2003 – 2016: Режим доступа: http://www.intuit.ru/studies/courses/10/10/info/, свободный. - Загл. с экрана (дата обращения: 17.11.2016).	http://www.intuit.ru/studies/courses/10/10/info	основные понятия ИБ, структура мер в области ИБ, меры законодательного, административного, процедурного и программно-технического обеспечения ИБ
---	---	---

Таблица 3 – Дополнительная литература

Библиографическое описание* издания (автор, наименование, вид, место и год издания, кол. стр.)	Кол. экз. в библ. НовГУ	Наличие в ЭБС
Жгун Т.В. Методы защиты информации.. [Электронный ресурс]: конспект лекций. – Великий Новгород, 2014. – 171 с. – Режим доступа: https://novsu.bibliotech.ru/Catalog/Index		да
Жгун Т.В. Методы защиты информации. Методические указания к выполнения лабораторных работ. [Электронный ресурс] : методические указания . – Великий Новгород, 2013. – 40 с. – Режим доступа: https://novsu.bibliotech.ru/Catalog/Index		да
Жгун Т.В. Методы защиты информации. Методические указания к практическим занятиям. [Электронный ресурс] : методические указания . – Великий Новгород, 2013. – 64 с. – Режим доступа: https://novsu.bibliotech.ru/Catalog/Index		да
Рябко Б.Я. Криптографические методы защиты информации : учеб. пособие для вузов. - М. : Горячая линия-Телеком, 2005. - 229с. Ф1-3	3	
Рябко Б.Я. Основы современной криптографии для специалистов в информационных технологиях / РАН,Ин-т вычисл.технологий;Сиб.гос.ун-т телекоммуникаций и информатики. - М. : Научный мир, 2004. - 172с. – Ф1-4	4	
Молдовян Н.А. Введение в криптосистемы с открытым ключом : Учеб.пособие. - СПб. : БХВ-Петербург, 2005. - 286с.-(Ф1-5	5	

Действительно для учебного года _____ / _____

Зав. кафедрой _____
подпись И.О.Фамилия

_____ 20..... г.

СОГЛАСОВАНО

НБ НовГУ:

_____ должность _____ подпись _____ расшифровка

Банк заданий для оценочного средства №1 «Домашнее задание 1»**Задание 1**

Зашифровать сообщение с помощью маршрутной транспозиции с помощью двойной перестановки строк и столбцов, определяемой паролем. Выбор открытого текста осуществляется по табл.1 в соответствии с номером студента в списке группы. Пароль выбирается из этой же таблицы. Размер таблицы для шифрования 5×6. Первые 5 различных символов пароля служат для перестановки столбцов, 6 следующих символов служат для перестановки строк.

$$P = N; \quad K = 26 - N$$

В пароле используются только неповторяющиеся символы.

Задание 2

С помощью «квадрата Полибия» зашифровать сообщение. Выбор открытого текста осуществляется по табл.1 в соответствии с номером студента в списке группы. Пароль выбирается из этой же таблицы. Размер таблицы для шифрования 5×6.

$$P = N; \quad K = 26 - N$$

В пароле используются только неповторяющиеся символы.

Таблица 1 – Выбор открытого текста для шифрования

№	Открытый текст
1	Повадится овца не хуже козы
2	Не робей, воробей, держись орлом.
3	Не разводи усок на чужой кусок
4	Сурьма косых глаз не исправит.
5	сухой по мокрому не тужит.
6	Повадится овца не хуже козы.
7	Повадки волчьи, а душа заячья
8	По хозяину и собаке честь.
9	Поздно шуке на сковороде вспоминать о воде.
10	Поле глазасто, а лес ушаст.
11	Порозно думать вместе не жить
12	Посуленному только дурак рад.
13	Промеж худых и хорошему плохо..
14	Проживет Фаддей и без затей
15	Пуст мешок стоять не будет.
16	Под каждой крышей свои мыши
17	Пустой колос голову кверху носит.
18	Порозно думать вместе не жить
19	Родной куст и зайцу дорог.
20	Спесь росту не прибавит.
21	Не пойман-не вор, не уличена - не гулена.
22	Не разводи усок на чужой кусок
23	сухой по мокрому не тужит
24	Не робей, воробей, держись орлом.
25	Повадки волчьи, а душа заячья

Задание 3

С помощью шифра Вижинера зашифровать сообщение. Выбор открытого текста осуществляется по табл.1 в соответствии с номером студента в списке группы. Пароль выбирается из этой же таблицы.

$$P = N$$

$$K = 26 - N$$

Задание 4

С помощью шифра Пфайфера зашифровать сообщение. Выбор открытого текста осуществляется по табл.1 в соответствии с номером студента в списке группы. Пароль выбирается из этой же таблицы. Размер таблицы для шифрования 5×6.

$$P = N \quad K = 26 - N$$

В пароле используются только неповторяющиеся символы. Длина пароля 7 символов. Разделителем служит символ «х».

Таблица 2 – Таблица Вижинера

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а
в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б
г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в
д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г
е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д
ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е
з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з
й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и
к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л
н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м
о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н
п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о
р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с
у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т
ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ
ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы
э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь
ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э
я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю

Банк заданий для оценочного средства №2 «Домашнее задание 2»

Задание 1

Вычислить 2 итерации, используя сеть Файстеля. Размер блока - 4 бита. С качестве нелинейной функции А использовать инверсию элементов блока. Открытый текст и ключ выбираем в таблице 3. в соответствии с номером студента в списке группы.

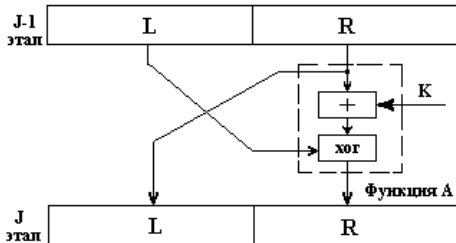


Таблица 3 – Открытый текст и ключ

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Открытый текст	5	8	7	4	11	13	6	10	14	6	2	15	5	8	7	4	11	13	6	10	14	6	2	15	4
Ключ	4	11	13	6	10	14	6	2	15	5	8	7	4	11	13	6	10	14	6	2	15	4	15	5	8

Задание 2

Вычислить 1 итерацию алгоритма DES. Размер блока - 64 бита. Открытый текст – строка из нулей. Ключ выбираем в таблице 3 в соответствии с номером студента в списке группы.

Таблица 4 – Ключ

№	1	2	3	4	5	6	7	8	9	10	11	12	13
Ключ	2^{16+2}	$2^{16+2^{15}}$	2^{16}	2^{15+2}	1	2^{15}	2^{16+2}	$2^{16+2^{15}}$	2^{16}	2^{15+2}	1	2^{15}	2^{16+2}
№	14	15	16	17	18	19	20	21	22	23	24	25	
Ключ	$2^{16+2^{15}}$	2^{16}	2^{15+2}	1	2^{15}	2^{16+2}	$2^{16+2^{15}}$	2^{16}	2^{15+2}	1	2^{15}	2^{16+2}	

Таблица 5 – Вычисление ключей в алгоритме DES.

(а) перестановка со сжатием

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

(в) таблица сдвигов влево

Номер раунда	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Число сдвигов	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Таблица 6 - Определение S-матриц алгоритма DES.

S1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	12	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Таблица 7 (а) начальная перестановка IP (б) перестановка, обратная начальной IP^{-1}

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

	40	8	48	16	56	24	64	32
	39	7	47	15	55	23	63	31
	38	6	46	14	54	22	62	30
	37	5	45	13	53	21	61	29
	36	4	44	12	52	20	60	28
	35	3	43	11	51	19	59	27
	34	2	42	10	50	18	58	26
	33	1	41	9	49	17	57	25

(в) перестановка с расширением E (г) перестановка P

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	27
28	29	30	31	32	1

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Задание 3

Вычислить 1 итерацию алгоритма ГОСТ. Размер блока - 64 бита. Открытый текст – строка из нулей. Ключ выбираем в таблице 3 в соответствии с номером студента в списке группы.

Таблица 8 – Выбор ключа

№	1	2	3	4	5	6	7	8	9	10	11	12	13
Ключ	2^{16+2}	$2^{16+2^{15}}$	2^{16}	2^{15+2}	1	2^{15}	2^{16+2}	$2^{16+2^{15}}$	2^{16}	2^{15+2}	1	2^{15}	2^{16+2}
№	14	15	16	17	18	19	20	21	22	23	24	25	
Ключ	$2^{16+2^{15}}$	2^{16}	2^{15+2}	1	2^{15}	2^{16+2}	$2^{16+2^{15}}$	2^{16}	2^{15+2}	1	2^{15}	2^{16+2}	

Таблица 9 – S-box алгоритма ГОСТ.

Номер S-блока	Значение
1	4 10 9 2 13 8 0 14 6 11 1 12 7 15 5 3
2	14 11 4 12 6 13 15 10 2 3 8 1 0 7 5 9
3	5 8 1 13 10 3 4 2 14 15 12 7 6 0 9 11
4	7 13 10 1 0 8 9 15 14 4 6 12 11 2 5 3
5	6 12 7 1 5 15 13 8 4 10 9 14 0 3 11 2
6	4 11 10 0 7 2 1 13 3 6 8 5 9 12 15 14
7	13 11 4 1 3 15 5 9 0 10 14 7 6 8 2 12
8	1 15 13 0 5 7 10 4 9 2 3 14 6 11 8 12

Задание 4

Вычислить дискретный логарифм элемента поля. Выбор поля и элемента осуществляется по табл.2 в соответствии с номером студента в списке группы. Пароль выбирается из этой же таблице.

Таблица 10 – Выбор конечного поля и элемента

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Поле GF	2^4	3^3	5^2	47	2^4	3^3	5^2	47	2^4	3^3	5^2	47	2^4	3^3	5^2	47	2^4	3^3	5^2	47	2^4	3^3	5^2	47	2^4
Элемент	54	47	32	64	74	54	47	32	64	74	54	47	32	64	74	54	47	32	64	74	54	47	32	64	74

Действительно для учебного года _____/_____

Зав. кафедрой _____
подпись И.О.Фамилия

_____ 20..... г.

СОГЛАСОВАНО

НБ НовГУ:

_____ должность _____ подпись _____ расшифровка

ПРИЛОЖЕНИЕ Е**КОНТРОЛЬНЫЕ ВОПРОСЫ К ЭКЗАМЕНУ ПО ДИСЦИПЛИНЕ
«МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ».**

- 1 Основные понятия и определения информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности. Классификация атак. Модели сетевой безопасности и безопасности информационной системы.
- 2 Классическая задача криптографии. Угрозы со стороны злоумышленника и участников процесса информационного взаимодействия.
- 3 Шифры замены и перестановки. Моно- и многоалфавитные подстановки Шифры Цезаря, Виженера, Вернама. Методы дешифрования.
- 4 Классификация методов дешифрования. Модель предполагаемого противника. Правила Керкхоффа.
- 5 Совершенная секретность по Шеннону. Примеры совершенно секретных систем. Шифр Вернама. Понятие об управлении ключами.
- 6 Блочные криптосистемы с секретным ключом. Алгоритм DES. Описание DES. Основные этапы алгоритма.
- 7 Схема алгоритма DES. Раунд алгоритма. Преобразование ключа.
- 8 Алгоритм DES. Подстановка с помощью S-блоков. Расшифрование в DES.
- 9 Блочные криптосистемы с секретным ключом. Режимы работы. ГОСТ 28147-89 в режиме простой замены.
- 10 Поточные криптосистемы с секретным ключом. Синхронные и самосинхронизирующиеся поточные криптосистемы. Примеры. ГОСТ 28147-89 в режимах гаммирования.
- 11 Стандарт криптографической защиты 21 века (AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра.
- 12 Теория сложности вычислений. Классификация алгоритмов.
- 13 Алгоритм RSA. Математическая модель алгоритма. Стойкость алгоритма.
- 14 Криптосистема Эль-Гамала.
- 15 Электронная подпись. Варианты электронной подписи на основе алгоритмов RSA и Эль-Гамала.
- 16 Хэш-функции и их применение. Хеш-функция MD2.
- 17 Однонаправленные (односторонние) функции с секретом и их применение.
- 18 Обобщенная модель электронной цифровой подписи. Схема Диффи-Хеллмана, схема Эль-Гамала.
- 19 Цифровая подпись на основе алгоритма RSA.
- 20 Стандарт цифровой подписи DSS. Генерация цифровой подписи. Проверка цифровой подписи.
- 21 Основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны. Протоколы аутентификации с использованием nonce и временных меток.
- 22 Криптографические протоколы. Понятие криптографического протокола и обоснование необходимости их использования. Протокол обмена сеансовыми ключами. Вскрытие "человек-в-середине". Протокол "держась за руки".
- 23 Сертификация ключей с помощью цифровых подписей. Разделение секрета. Метки времени. Пример протокола защиты базы данных.
- 24 Основы криптоанализа. Обзор возможных вариантов криптоанализа. Метод вскрытия «встреча посередине». Вскрытие со словарем. Вскрытие системы Виженера, использующей простой XOR. Метод бесключевого чтения RSA. Атака на подпись RSA по выбранному шифротексту. Вскрытие хэш-функций с использованием парадокса дня рождения.
- 25 Криптосистемы на эллиптических кривых.

Примерный вариант билета
по дисциплине «Методы и средства защиты информации»

1. . Решить в $GF(2^3)$ систему
$$\begin{cases} 2x + y = 3 \\ x + 2y = 2 \end{cases}$$

2. Выработать секретный ключ по алгоритму Диффи-Хеллмана с абонентом В, который задумал секретное число 3. Открытый ключ $(17, q)$, где q – примитивный элемент поля $GF(17)$.

3. Блочные криптосистемы с секретным ключом. Режимы работы. ГОСТ 28147-89 в режиме простой замены.

ПРИЛОЖЕНИЕ Ж
СПИСОК ВОЗМОЖНЫХ ВОПРОСОВ ДЛЯ СОБЕСЕДОВАНИЯ ПО
ЛАБОРАТОРНЫМ РАБОТАМ

Собеседование по 1й лабораторной работе

1. Какой шифр называется шифром подстановки?
2. Какой шифр называется шифром перестановки?
3. Какой шифр называется поворотной решеткой?
4. Какой шифр называется шифром вертикальной перестановки?
5. К какому классу шифров относится шифр Цезаря?
6. Что такое гамма и гаммирование?
7. В чем заключается шифрование по Вижинеру?

Собеседование по 2й лабораторной работе

1. Что называется ключом шифрования.
2. Какие шифры называются шифрами на открытом ключе и какие – шифрами на секретном ключе?
3. Ответ : в шифрах на секретном ключе один и тот же ключ используется как для шифрования, так и для дешифрования данных. В шифрах на открытом ключе при шифровании и дешифровании используются разные ключи: открытый и общеизвестный – при шифровании, закрытый, секретный – при дешифровании.
4. Чем отличается поточное шифрование от блочного?
5. Чему равна длина секретного ключа алгоритма DES?
6. Чему может быть равна длина секретного ключа алгоритма Rijndael?
7. Какая архитектура лежит в основе алгоритма DES?
8. Какой параметр определяет криптостойкость современного алгоритма?
9. Что такое ECB, CBC

Собеседование по 3й лабораторной работе

1. Какая процедура является более производительной – асимметричное шифрование/ дешифрование или симметричное шифрование/дешифрование?
2. К какому типу криптоалгоритма (с точки зрения его устойчивости к взлому) и почему относится алгоритм RSA?
3. Какая трудноразрешимая математическая задача лежит в основе стойкости алгоритма RSA?
4. Какая трудноразрешимая математическая задача лежит в основе стойкости алгоритма Эль Гамаль?
5. В чем заключается проблема дискретного логарифма?
6. В чем заключаются проблемы разложения больших чисел на простые множители и вычисления корней алгебраических уравнений?

Собеседование по 4й лабораторной работе

1. Что называется ключом шифрования.
2. Какие шифры называются шифрами на открытом ключе и какие – шифрами на секретном ключе?
3. Чем отличается поточное шифрование от блочного?
4. Чему равна длина секретного ключа алгоритма DES?
5. Чему может быть равна длина секретного ключа алгоритма Rijndael? Какая архитектура лежит в основе алгоритма DES?
6. Какой параметр определяет криптостойкость современного алгоритма?
7. Что такое ECB, CBC

Собеседование по 5й лабораторной работе

1. Что такое хэш-функция? Зачем она нужна?
2. Что называется электронной цифровой подписью?
3. Для чего используется ЭЦП?
4. ЭЦП используется для аутентификации отправителя сообщений и того, чтобы сделать сообщение неотвержаемым?
5. Что такое дайджест-сообщение?
6. Что такое вычислительно необратимая функция?