Министерство образования и науки РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «АмГУ»)

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
(наименование учебной дисциплины/модуля)

сборник учебно-методических материалов

для специальности 09.03.02 «Информационные системы и технологии»
(наименование учебной дисциплины/модуля)

Направленность (профиль) / специализация образовательной программы «Безопасность информационных систем»

Благовещенск 2017 г.

Печатается по решению редакционно-издательского совета факультета математики и информатики *Амурского государственного университета*

Составитель: Семичевская Н. П.

Криптографические методы защиты информации: сборник учебно-методических материалов для специальности 09.03.02. – Благовещенск: Амурский гос. ун-т, 2017.

СОДЕРЖАНИЕ

1. КРАТКОЕ ИЗЛОЖЕНИЕ ЛЕКЦИОННОГО МАТЕРИАЛА

Содержание курса лекций

Темы лекций	Содержание лекции (план лекции)
1	2
Раздел 1 Основные понятия и задачи криптографии **Тема1.** Докомпьютерная и компьютерная криптография.	История криптографии. Докомпьютерная и компьютерная криптография. Простейшие исторические шифры и их анализ. Классификаторы в криптографии. Основные понятия и задачи криптографии Основные понятия криптологии. Основные понятия криптографии: математическая формализация. Симметричные, асимметричные шифрсистемы. Понятие о криптографических системах: (Криптосистема RSA) Математическая модели открытых текстов. Критерии на открытый текст. Понятие шифра, модель шифра. Классификация шифров. Понятие цифровой подписи.
Тема2. Основные понятия и задачи криптографии	Простейшие шифры замены и их анализ. Шифры замены: шифр Цезаря, таблица Вижинера, шифр пропорциональной замены, замена биграмм. Простейшие шифры перестановки и их анализ. Шифры перестановки: шифрование с помощью скиталя, маршрутные шифры, решетка Кардано; Шифры гаммирования и их анализ. Дисковые шифраторы многоалфавитной замены.
Тема3. Шифры замены, перестановки, гаммирования.	Обзор криптографических методов защиты информации. Ключевая система шифра. Генерация ключей. Обеспечение секретности ключей (схемы разделения секрета; рассылка, хранение, смена ключей). Понятие и примеры криптографических протоколов.
Раздел 2 Методы шифрования **Тема4.** Обзор криптографических методов защиты информации. Понятие и примеры криптографических протоколов.	Криптографическая стойкость шифра (вероятностные модели шифра, совершенно стойкие шифры, оценка практической стойкости шифров). Алгоритм шифрования DES и ее свойства. Основные задачи защиты информации криптографическими методами. Надежность шифров. Практическая стой-

Темы лекций	Содержание лекции (план лекции)
	кость шифров. Метод тотального опробования ключей. Вопросы имитозащиты шифров. Коды аутентификации. Помехоустойчивость шифров. Теорема Маркова.
Тема5. Алгоритм шифрования DES и ее свойства.	Примеры криптографических систем Алгоритмы криптографических систем. Криптосистема DES и ее свойства.
Тема6. Криптосистема IDEA.	Криптосистема IDEA и ее свойства. Алгоритм Rijndael.
Раздел 3 Примеры криптографических систем **Тема7.** ГОСТы в криптографии зарубежной и отечественной.	ГОСТы в криптографии зарубежной и отечественной.
Тема8. Криптосистема RSA и ее анализ.	Криптосистемы на основе открытого ключа. Вычислительно сложные задачи математики. Криптосистема RSA и ее анализ.
Тема9. Шифросистема Эль Гамаля. Схемы цифровой подписи.	Криптосистема Эль-Гамаля, Мак-Эллиса, Меркля-Хеллмана. Шифрсистема Эль Гамаля. Схемы цифровой подписи.

В процессе изучения лекционного материала *рекомендуется пользоваться* учебной литературой, представленной в разделе учебно-методическое и информационное обеспечение дисциплины (модуля) рабочей программы дисциплины.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНЫМ ЗАНЯТИЯМ

Тематический план лабораторного практикума дисциплины

№ Лаб. работы	Темы занятий	Задание и контрольные вопросы
№1	Алгоритмы простой замены (Таблицы замены)	**Задание** **1.** Изучить криптографический алгоритм простой замены. **2.** Сформировать таблицы замены в редакторе электронных таблиц.

		3. Оформить электронный отчет по лабораторной работе с ответами на контрольные работы. **4.** Сформировать систему криптографической защиты. **Контрольные вопросы** **1.** К какому классу криптографических систем относится алгоритм? 2. Какова стойкость криптографического алгоритма? 3. Перечислить основные компоненты системы криптографической защиты.
№2	Шифрование/расшифрование по Вижинеру	**Задание** **1.** Изучить криптографический алгоритм простой замены. **2.** Сформировать таблицы замены в редакторе электронных таблиц. **3.** Оформить электронный отчет по лабораторной работе с ответами на контрольные работы. **4.** Сформировать систему криптографической защиты. **Контрольные вопросы** **1.** К какому классу криптографических систем относится алгоритм? 2. Какова стойкость криптографического алгоритма? **3.** Перечислить основные компоненты системы криптографической защиты.
№3	Простейшие шифры перестановки	**Задание** 1. Изучить криптографический алгоритм шифра перестановки. 2. Сформировать шифросистему в редакторе электронных таблиц. 3. Оформить электронный отчет по лабораторной работе с ответами на контрольные работы. 4. Сформировать систему криптографической защиты. **Контрольные вопросы** **1.** К какому классу криптографических систем относится алгоритм? 2. Какова стойкость криптографического алгоритма? **3.** Перечислить основные компоненты си-

		стемы криптографической защиты.
№4	Шифры гаммирования	**Задание** 1. Изучить криптографический алгоритм шифра гаммирования. **2.** Сформировать шифросистему в редакторе электронных таблиц. **3.** Оформить электронный отчет по лабораторной работе с ответами на контрольные работы. **4.** Сформировать систему криптографической защиты. **Контрольные вопросы** **1.** К какому классу криптографических систем относится алгоритм? 2. Какова стойкость криптографического алгоритма? **3.** Перечислить основные компоненты системы криптографической защиты.
№5	Программирование простейших алгоритмов в криптографии (Алгоритм Евклида, инверсия, расчет секретной экспоненты)	**Задание** 1. Изучить криптографические алгоритмы. **2.** Запрограммировать алгоритмы на языках высокого уровня. **3.** Оформить электронный отчет по лабораторной работе с ответами на контрольные работы. **4.** Сформировать систему криптографической защиты, с использованием изученных алгоритмов. **Контрольные вопросы** **1.** К какому классу криптографических систем относится алгоритм? 2. Какова стойкость криптографического алгоритма? **3.** Перечислить основные компоненты системы криптографической защиты.
№6	Реализация системы шифрования по ГОСТ 28147-89.	**Задание** 1. Изучить криптографический алгоритм системы шифрования по ГОСТ 28147-89. **2.** Запрограммировать алгоритм на языках высокого уровня. **3.** Оформить электронный отчет по лабораторной работе с ответами на контрольные работы. **4.** Сформировать систему криптографической защиты, с использованием алгоритма

		системы шифрования по ГОСТ 28147-89. **Контрольные вопросы** **1.** К какому классу криптографических систем относится алгоритм? 2. Какова стойкость криптографического алгоритма? 3. Какие элементы криптоанализа используются для системы шифрования? **4.** Перечислить основные компоненты системы криптографической защиты.
№7	Реализация системы шифрования RSA	**Задание** 1. Изучить криптографический алгоритм системы шифрования **RSA**. **2.** Запрограммировать алгоритм на языках высокого уровня. **3.** Оформить электронный отчет по лабораторной работе с ответами на контрольные работы. **4.** Сформировать систему криптографической защиты, с использованием алгоритма системы шифрования RSA. **Контрольные вопросы** **1.** К какому классу криптографических систем относится алгоритм? 2. Какова стойкость криптографического алгоритма? 3. Какие элементы криптоанализа используются для системы шифрования? 4. Перечислить основные компоненты системы криптографической защиты.
№8	Реализация системы шифрования ЭльГамаля.	**Задание** 1. Изучить криптографический алгоритм системы шифрования ЭльГамаля. **2.** Запрограммировать алгоритм на языках высокого уровня. **3.** Оформить электронный отчет по лабораторной работе с ответами на контрольные работы. **4.** Сформировать систему криптографической защиты, с использованием алгоритма системы шифрования ЭльГамаля. **Контрольные вопросы** **1.** К какому классу криптографических систем относится алгоритм? 2. Какова стойкость криптографического ал-

		горитма? 3. Какие элементы криптоанализа используются для системы шифрования? **4.** Перечислить основные компоненты системы криптографической защиты.
№9	Реализация схемы цифровой подписи.	**Задание** 1. Изучить криптографический алгоритм схемы цифровой подписи. **2.** Запрограммировать алгоритмы на языках высокого уровня. **3.** Оформить электронный отчет по лабораторной работе с ответами на контрольные работы. 4. Сформировать систему криптографической защиты, с использованием схемы цифровой подписи. **Контрольные вопросы** **1.** К какому классу криптографических систем относится алгоритм? 2. Перечислить основные компоненты системы криптографической защиты.

Методические указания к лабораторным занятиям

Общие положения. В процессе выполнения лабораторного практикума студенту предлагается выполнить задание к лабораторной работе и ответить на ряд контрольных вопросов (в письменной или устной форме). Письменную форму ответа необходимо оформлять в виде отчета по лабораторной работе в бумажной или электронной форме.

Студенты на лабораторном практикуме должны продемонстрировать свои навыки решения стандартных задач теории, программирования алгоритмов шифросистем криптографии и умения применять стандартные алгоритмические структуры при разработке программ и программных комплексов, используемых в информационных системах.

Содержание отчета по лабораторной работе

В отчете к лабораторной работе необходимо представить краткое изложение теоретического материала, листинг программы и алгоритмические

структуры, разработанные в ходе выполнения лабораторной работы, а также ответы на контрольные вопросы, предложенные преподавателем.

При выполнении лабораторных работ необходимо использовать стандартные среды программирования.

Для подготовки к лабораторной работе *рекомендуется пользоваться* учебной литературой, представленной в разделе учебно-методическое и информационное обеспечение дисциплины (модуля) рабочей программы дисциплины.

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

Темы практических занятий	**Задания и контрольные вопросы**
Практическое занятие №1 Основные понятия криптографии: математическая формализация.	**Задания** 1. Изучить основные понятия криптографии: математическая формализация **Контрольные вопросы** **1.** Какие официальные источники Российского законодательства в области информации, информационных технологий и защиты информации вы знаете? 2.Какие международные законодательные акты существуют в области информации, информационных технологий и защиты информации 3. Перечислить основные компоненты системы Российского законодательства в области информации, информационных технологий и защиты информации. 4. На каком уровне системы Российского законодательства находятся Федеральные законы? 5. На каком уровне системы Российского законодательства находятся Кодексы РФ?
Практическое занятие №2 Элементы теории чисел. Основные теоремы теории чисел.	**Задания** 1. Изучить элементы теории чисел. Основные теоремы теории чисел. **Контрольные вопросы** **1.** Какие Статьи Гражданского кодекса РФ в области ИТ и ИБ вы знаете? 2. Перечислить основные критерии в области информации, информационных технологий и за-

	щиты информации в ГК РФ. 3. В каких статьях ГК РФ представлен материал по информационной безопасности и защите информации, включая и государственную тайну?
Практическое занятие №3 Вычислительная сложность в математике. Вычислительно сложные задачи криптографии.	**Задания** 1. Изучить раздел математики, связанный с вычислительной сложностью. 2. Изучить признаки делимости. 3. Изучить алгоритмы проверки на простоту. **Контрольные вопросы** **1.** Какие Статьи Кодекса об административных правонарушениях РФ в области ИТ и ИБ вы знаете? 2. Перечислить основные критерии защиты в области информации, информационных технологий и защиты информации в КоАП РФ. 3. В каких статьях КоАП РФ представлен материал по информационной безопасности и защите информации, включая и государственную тайну ?
Практическое занятие №4 Простейшие шифры замены и их анализ.	**Задания** 1. Изучить простые шифры замены и ее криптоанализ. **Контрольные вопросы** **1.** Какие Статьи Уголовного Кодекса РФ в области ИТ и ИБ вы знаете? 2. Перечислить основные критерии защиты в области информации, информационных технологий и защиты информации в УК РФ. 3. В каких статьях УК РФ представлен материал по информационной безопасности и защите информации, включая и государственную тайну?
Практическое занятие №5 Простейшие шифры перестановки и их анализ.	**Задания** 1. Изучить простые шифры перестановки и ее криптоанализ. **Контрольные вопросы** 1. Перечислить основные критерии защиты в области информации, информационных технологий и защиты информации в № 149 – ФЗ «Об информации, информационных технологиях и защите информации». 2. В каких статьях № 149 – ФЗ «Об информации, информационных технологиях и защите информации» представлен материал по информационной безопасности и защите информации, включая и государственную тайну?

Практическое занятие №6 Шифры гаммирования и их анализ.	**Задания** 1. Изучить шифры гаммирования и ее криптоанализ. **Контрольные вопросы** 1. Перечислить основные критерии защиты в области информации, информационных технологий и защиты информации в № 152 – ФЗ «О персональных данных». 2. В каких статьях № 152 – ФЗ «О персональных данных» представлен материал по информационной безопасности и защите информации, включая и государственную тайну?
Практическое занятие №7 Алгоритм национального стандарта ГОСТ 28147-89	**Задания** 1. Найти официальные источники Российские государственные стандарты для унифицированного алгоритмического обеспечения средств криптографической защиты. 2. Изучить структуру государственного стандарта для унифицированного алгоритмического обеспечения средств криптографической защиты ГОСТ 28147-89. **Контрольные вопросы** 1. Перечислить основные критерии защиты в области информации, информационных технологий и защиты информации в № 63 – ФЗ «Об электронной подписи». **2.** В каких статьях № 63 – ФЗ «Об электронной подписи» представлен материал по информационной безопасности и защите информации, включая и государственную тайну?
Практическое занятие №8 Криптосистема RSA и ее анализ.	**Задания** 1. Изучить криптосистему RSA и ее криптоанализ. **Контрольные вопросы** 1. Перечислить основные критерии защиты в области информации, информационных технологий и защиты информации. 2. В каких статьях представлен материал по информационной безопасности и защите информации, включая и государственную тайну?
Практическое занятие №9 Шифрсистема ЭльГамаля. Схемы цифровой подписи.	**Задания** 1.Изучить структуру шифрсистему ЭльГамаля. Схема цифровой подписи. **Контрольные вопросы**

	1. Перечислить основные критерии защиты в области информации, информационных технологий и защиты информации. 2. В каких статьях представлен материал по информационной безопасности и защите информации, включая и государственную тайну?
Подготовка к экзамену (решение экзаменационных задач)	**Задания** 1. Изучить структуру унифицированного алгоритмического обеспечения средств криптографической защиты. 2. Научиться решать стандартные задачи криптографии.

Методические указания к практическим занятиям

Общие положения. В процессе обучения на практическом занятии студенту предлагается выполнить серию практических заданий и ответить на ряд контрольных вопросов в устной форме.

Студенты при проведении практического занятия должны приобрести знания основных положений и понятия криптографии и изучить теорию криптографических методов защиты информации, а также и рассмотреть примеры реализации криптографических методов защиты информации на практике при защите в информационных системах и сформировать устойчивые навыки практического использования криптографических методов защиты информации.

Практические занятия по дисциплине основаны на материале системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов в информационных системах.

Для выполнения заданий на практических занятиях *рекомендуется пользоваться* учебной литературой, представленной в разделе учебно-методическое и информационное обеспечение дисциплины (модуля) рабочей программы дисциплины.

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Тематика разделов самостоятельной работы		Методические указания для самостоятельной работы студентов	Методическое обеспечение
Домашние задания по темам			
1	Элементы теории чисел. Основные теоремы теории чисел.	При подготовке к практической работе рекомендуется использовать теоретический материал по теории чисел.	1. Лось, А. Б. Криптографические методы защиты информации: учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М. : Издательство Юрайт, 2017. 2. Горбунов, В.А. Математические методы в теории защиты информации [Электрон-ный ресурс] / В.А. Горбунов. – СПб.: Изд-во Московского Горного ун-та, 2004. – 82 с. (ЭБС Лань) 3. Глухов, М.М. Введение в теоретико-числовые методы криптографии [Электронный ресурс] / М.М. Глухов [и др.]. – СПб.: Лань, 2011. – 400 с. (ЭБС Лань)
2	Вычислительная сложность в математике. Вычислительно сложные задачи криптографии.	При подготовке к практической работе рекомендуется использовать классические методы криптографии и теоретический материал по математическим основам криптографии.	
3	Простейшие шифры замены и их анализ.	При подготовке к практической работе рекомендуется использовать материал лекций №2 и №3	
4	Простейшие шифры перестановки и их анализ.	При подготовке к практической работе рекомендуется использовать материал лекции №4 и результаты, полученные на лабораторном практикуме №3	
5	Шифры гаммирования и их анализ.	При подготовке к практической работе рекомендуется использовать материал лекции №3 и результаты, полученные на лабораторном практикуме №2	
6	Алгоритм национального стандарта-ГОСТ 28147-89	При подготовке к практической работе рекомендуется использовать материал лекций №5 и 6.	

7	Криптосистема RSA и ее анализ.	При подготовке к практической работе рекомендуется использовать материал лекций №7.	
8	Шифрсистема ЭльГамаля. Схемы цифровой подписи.	При подготовке к практической работе рекомендуется использовать материал лекций №8 и 9.	
Подготовка к лабораторному практикуму			
1	Программирование простейших алгоритмов в криптографии (Алгоритм Евклида, инверсия, расчет секретной экспоненты)	При подготовке к практической работе рекомендуется использовать теоретический материал по теории чисел и материал лекций №7,8.	1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М. : Издательство Юрайт, 2017. —312 с. — (Серия : Специалист). — ISBN 978-5-9916-9043-0. — Режим доступа : www.biblio-online.ru/book/E458AFCD-826E-4A1F-9BAB-68BB83EA616F
2	Реализация системы шифрования по ГОСТ 28147-89 в среде программирования	При подготовке к практической работе рекомендуется использовать материал лекций №5 и 6.	
3	Реализация системы шифрования RSA	При подготовке к практической работе рекомендуется использовать материал лекций №7.	
4	Реализация системы шифрования ЭльГамаля.	При подготовке к практической работе рекомендуется использовать материал лекции №8.	
5	Реализация схемы цифровой подписи.	При подготовке к практической работе рекомендуется использовать материал лекции №9.	

Тематический план контрольных работ	**Методические указания для подготовки к контрольным работам студентов**

Тематический план контрольных работ	Методические указания для подготовки к контрольным работам студентов
Контрольная работа №1 «Обобщенный алгоритм Евклида»	При подготовке к контрольной работе рекомендуется использовать материал практического занятия №1
Контрольная работа №2 «Алгоритмы простой перестановки и замены»	При подготовке к контрольной работе рекомендуется использовать классические методы криптографии и материал лабораторных работ №1 и №2
Контрольная работа №3 «Критерии простоты чисел»	При подготовке к контрольной работе рекомендуется использовать теорию чисел и материал практических работ №3 и №4
Контрольная работа №4 «Операции над большими простыми числами»	При подготовке к контрольной работе рекомендуется использовать материалы практических занятий №3 и №4
Контрольная работа №5 «Расчет параметров алгоритма RSA»	При подготовке к контрольной работе рекомендуется использовать классический метод криптографии и материал лабораторной работы №6

Примерные контрольные вопросы к блиц-опросам

Контрольные вопросы к блиц-опросу №1

5. Какие предпосылки исторического развития криптографии привели к развитию компьютерной криптографии?
6. Раскрыть основной принцип шифрования заменой.
7. Проверить числа n и m на взаимную простоту.

Контрольные вопросы к блиц-опросу №2

1. Дать определение шифросистемы.
2. Описать схему шифра простой замены ШПЗ.
3. Какие признаки делимости чисел вам известны?

Контрольные вопросы к блиц-опросу №3

1. Какие шифросистемы используются на современном этапе?
2. Указать достоинства и недостатки алгоритма RSA.
3. Зашифровать свою фамилию, используя параметры открытого ключа алгоритма RSA.

Общие положения. Самостоятельная работа студента представляет собой все виды самостоятельной работы, выполняемые в учебных аудиториях и дома.

Для выполнения самостоятельной работы *рекомендуется пользоваться* учебной литературой, представленной в разделе учебно-методическое и информационное обеспечение дисциплины (модуля) рабочей программы дисциплины.

Подготовка к блиц опросам подразумевает изучение и использование лекционного материала в режиме короткого опроса на лекции, на блиц-опросе студент должен продемонстрировать и навыки решения небольших задач.

Выполнение самостоятельной работы при подготовке ко всем видам занятий студент может использовать следующие электронные библиотечные системы (ЭБС) в качестве информационного ресурса:

Наименование ресурса	**Краткая характеристика электронного ресурса**
http://www.iprbookshop.ru	ЭБС IPRbooks — научно-образовательный ресурс для решения задач обучения в России и за рубежом. Уникальная платформа ЭБС IPRbooks объединяет новейшие информационные технологии и учебную лицензионную литературу. Контент ЭБС IPRbooks отвечает требованиям стандартов высшей школы, СПО, дополнительного и дистанционного образования. ЭБС IPRbooks в полном объеме соответствует требованиям законодательства РФ в сфере образования
https://e.lanbook.com/	Электронно-библиотечная система ЛАНЬ
https://www.biblio-online.ru/	ЭБ «Юрайт» - электронная библиотека, которая соответствует всем обязательным требованиям министерства образования. В электронной библиотеке представлены все книги издательства Юрайт.
	Автоматизированная информационная библиотечная система «ИРБИС 64»
http://gostedu.ru/	ГОСТы, СНиПы, СанПИНы и другие об-

Наименование ресурса	Краткая характеристика электронного ресурса
	разовательные ресурсы