

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
Ярославский государственный университет им. П.Г.Демидова

УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ И
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки (специальность):

02.04.02 Фундаментальная информатика и информационные технологии

Образовательная программа

Искусственный интеллект и компьютерные науки

очная форма обучения

Составитель:

ТИМОФЕЕВ ЕВГЕНИЙ АЛЕКСАНДРОВИЧ, Д.Ф.-М.Н., ПРОФЕССОР
Ф-ТА ИВТ ЯРГУ ИМ. П.Г. ДЕМИДОВА

г. Ярославль

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основная литература:

1. Гашков, С. Б., Криптографические методы защиты информации : учеб. пособие для вузов / С. Б. Гашков, Э. А. Применко, М. А. Черепнев, М., Академия, 2010, 298с
2. Математические методы защиты информации / Яросл. гос. ун-т. Ч. 2 [Электронный ресурс] : метод. указания (сост. М. В. Краснов), Ярославль, ЯрГУ, 2011, 44с
3. Математические методы защиты информации / Яросл. гос. ун-т. Ч. 2 : метод. указания (сост. М. В. Краснов), Ярославль, ЯрГУ, 2011, 44с
4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина - 2-е изд., перераб. и доп. - М.: Радио и связь, 2001.-376с
5. Сمارт Н. Криптография: учебник: перевод с англ. - М.: Техносфера, 2006.-528с.

Дополнительная литература:

1. Введение в криптографию: Учебник / Под общ. ред. В.В. Яценко. - СПб.: Питер, 2001.-288с
2. Тимофеев Е.А. Защита информации в распределенных сетях: учебное пособие для вузов. - Ярославль.: ЯрГУ, 2001.-60с
3. Краснов М.В. Математические методы защиты информации и информационной безопасности: методические указания. - Ярославль.: ЯрГУ, 2004.-27с.
4. Завгородний В.И. Комплексная защита информации в компьютерных системах: учебное пособие. - М.: Логос, 2001.-263с.
5. Ярочкин В.И. Информационная безопасность: Учебное пособие для студентов непрофильных вузов. - М.: Международные отноше, 2000.-400с.
6. Основы криптографии: Учебное пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. - М.: Гелиос АРВ, 2001.-480с.
7. Петраков А.В. Основы практической защиты информации: Учебное пособие для вузов - 3-е изд. - М.: Радио и связь, 2001.-368с.

В разделе 6.1 приводятся сведения об учебной литературе: учебники, учебные пособия.

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине (модулю)

Также для подбора учебной литературы рекомендуется использовать широкий спектр интернет-ресурсов:

1. Личный кабинет (http://lib.uniyl.ac.ru/opac/bk_login.php) дает возможность получения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб. и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт меню «Электронный каталог»; пройти процедуру авторизации, выбрав вкладку «Авторизация», и заполнить представленные поля информации.

2. Электронная библиотека учебных материалов ЯрГУ

(http://www.lib.uni-yar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.

3. Электронная картотека «Книгообеспеченность»

(http://www.lib.uni-yar.ac.ru/opac/bk_bookreq_find.php) раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет.

4. Электронно-библиотечная система «Университетская библиотека online»

(www.biblioclub.ru) - электронная библиотека, обеспечивающая доступ к наиболее востребованным материалам-первоисточникам, учебной, научной и художественной литературе ведущих издательств (*регистрация в электронной библиотеке – только в сети университета. После регистрации работа с системой возможна с любой точки доступа в Internet.).

5 Информационная система "Единое окно доступа к образовательным ресурсам"

(<http://window.edu.ru/library>).

Целью создания информационной системы "Единое окно доступа к образовательным ресурсам" (ИС "Единое окно ") является обеспечение свободного доступа к интегральному каталогу образовательных интернет-ресурсов и к электронной библиотеке учебно-методических материалов для общего и профессионального образования.

Информационная система "Единое окно доступа к образовательным ресурсам" создана по заказу Федерального агентства по образованию в 2005-2008 гг. Главной разработчик проекта - Федеральное государственное автономное учреждение Государственный научно-исследовательский институт информационных технологий и телекоммуникаций (ФГАУ ГНИИ ИТТ "Информика") www.informika.ru.

ИС "Единое окно" объединяет в единое информационное пространство электронные ресурсы свободного доступа для всех уровней образования в России. ***Разделы этой системы:***

- ***Электронная библиотека*** – является крупнейшим в российском сегменте Интернета хранилищем полнотекстовых версий учебных, учебно-методических и научных материалов с открытым доступом. Библиотека содержит более 30 000 материалов, источниками которых являются более трехсот российских вузов и других образовательных и научных учреждений. Основу наполнения библиотеки составляют электронные версии учебно-методических материалов, подготовленные в вузах, прошедшие рецензирование и рекомендованные к использованию советами факультетов, учебно-методическими комиссиями и другими вузовскими структурами, осуществляющими контроль учебно-методической деятельности.
- ***Интегральный каталог образовательных интернет-ресурсов*** содержит представленные в стандартизированной форме метаданные внешних ресурсов, а также содержит описания полнотекстовых публикаций электронной библиотеки. Общий объем каталога превышает 56 000 метаописаний (из них около 25 000 - внешние ресурсы). Расширенный поиск в "Каталоге" осуществляется по названию, автору, аннотации, ключевым словам с возможной фильтрацией по тематике, предмету, типу материала, уровню образования и аудитории.
- ***Избранное***. В разделе представлены подборки наиболее содержательных и полезных, по мнению редакции, интернет-ресурсов для общего и профессионального образования.
- ***Библиотеки вузов***. Раздел содержит подборки сайтов вузовских библиотек, электронных каталогов библиотек вузов и полнотекстовых электронных библиотек вузов.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля), включая перечень информационных справочных систем (при необходимости)

1. Электронная библиотека учебных материалов ЯрГУ
(http://www.lib.uni-yar.ac.ru/opac/bk_cat_find.php).
2. Информационная система "Единое окно доступа к образовательным ресурсам"
(<http://www.edu.ru> (раздел Учебно-методическая библиотека) или по прямой ссылке <http://window.edu.ru/library>).
3. Электронно-библиотечная система «Университетская библиотека online»
(www.biblioclub.ru).

Перечень информационных технологий, используемых при изучении дисциплины, включая программное обеспечение

В процессе осуществления образовательного процесса используются:

- для формирования текстов материалов для промежуточной и текущей аттестации – программы Microsoft Office, издательская система LaTeX;
- компиляторы с высокоуровневых языков программирования;
- для поиска учебной литературы библиотеки ЯрГУ – Автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next").

**Учебно-методические указания и рекомендации
к изучению тем лекционных и практических занятий, самостоятельной
работе студентов
Очная форма обучения**

Содержание дисциплины

Наименование раздела дисциплины	Название темы с кратким содержанием
Раздел 1 Введение. Идея криптосистем открытого ключа	Зачем защищать информацию. Общая схема системы защиты информации. Возможности шифрования и криптоанализа. История защиты информации. Исторические системы (Цезарь, Хилл, аффинная), одно алфавитные и много алфавитные системы (система Плейфейра, Виженера, Бьюфорта)
Раздел 2. Модульная арифметика. Проверка чисел на простоту	Понятие полиномиального и неполиномиального алгоритма. Понятие NP полной задачи. Примеры задач, для которых нахождение " $y=f(x)$ " (x) является более легкой (полиномиальной) задачей, а обратная задача " $x=f(y)$ " (y) является труднорешаемой. Введение в модулярную арифметику. Нахождение мультипликативно обратного элемента. Основная теорема об остатках. Проверка чисел на простоту(тест на основе теоремы Эйлера, тест Соловея-Штрассена, тест Миллера-Рабина). Примеры.

Наименование раздела	Название темы с кратким содержанием
Раздел 3. Системы открытого ключа	<p>Рюкзачная криптосистема. Построение криптосистемы. Возможность криптоанализа. Примеры. Теория достижимости. Модификация рюкзачной криптосистемы. Примеры.</p> <p>Криптосистема RSA. Построение криптосистемы. Криптоанализ и факторизация. Примеры.</p> <p>Криптосистемы Эль-Гамала, Рабина, Вильямса, Уильямса. Построение криптосистемы. Примеры.</p>
Раздел 4. Симметричные криптосистемы	<p>DES. Построение криптосистемы.</p> <p>IDEA. Построение криптосистемы.</p> <p>Гост. Построение криптосистемы. и т.д.</p> <p>О выборе плохих ключей.</p>
Раздел 5. Электронная цифровая подпись	<p>Общая схема ЭЦП. Примеры.</p> <p>Описание хэш функции. Примеры.</p> <p>Схема ЭЦП RSA. Примеры.</p> <p>Схема ЭЦП Эль-Гамала. Примеры.</p> <p>Схема ЭЦП DSA. Примеры.</p> <p>Схема ГОСТ Р34.10-94. Примеры.</p> <p>Подделка ЭЦП Примеры.</p>
Раздел 6. Способы передачи ключей	<p>Diffie-Hellman. Примеры</p> <p>Hughes. Примеры</p> <p>протокол точка-точка.</p> <p>трехпроходный протокол Шамира.</p> <p>обмен зашифрованными ключами: базовый протокол EKE (реализация EKE с помощью RSA, Эль-Гамала, Diffie-Hellman.) Примеры</p>
Раздел 7. Потокковое кодирование	<p>Определения. Классификация поточных шифров (синхронные и самосинхронизирующиеся) Конгруэнтные генераторы и криптоанализ конгруэнтных генераторов. Регистры сдвига. Алгоритм A5. Алгоритм RC4. Алгоритм Seal. Алгоритм Wake. Примеры.</p>
Раздел 8. Разделение секрета, подсознательный канал.	<p>Криптография с несколькими открытыми ключами. Примеры</p> <p>Схема интерполяционных многочленов Лагранжа. Примеры</p> <p>Подсознательный канал (Ong-Schnorr-Shamir, Эль-Гамаль, DSA). Примеры</p> <p>Доказательство с нулевым знанием и т.д.</p>

Варианты контрольной работы.

1. Взломать рюкзачную криптосистему $B=(10,6,11)$
2. Использовать модификацию рюкзачной криптосистемы для создания эцп $m=37$ подписать $a=11$
3. Взломать аффинную криптосистему если известно, что 12 переходит в 15, а 11 переходит в 10 модуль равен 31
4. построить систему Хилла $d=2$

Вариант 2.

1. Взломать рюкзачную криптосистему $B=(12,7,11)$
2. Использовать модификацию рюкзачной криптосистемы для создания эцп $m=41$ подписать $a=10$
3. Взломать аффинную криптосистему если известно, что 11 переходит в 15, а 11 переходит в 21 модуль равен 31
4. построить систему Хилла $d=3$
5. построить четвертую модификацию рюкзака

Контрольная работа № 2:**Вариант 1.**

1. Построить систему RSA $p=11$, $q=13$
2. Построить систему Уильямса
3. Привести пример системы доказательства с нулевым знанием
4. Схема ЭЦП ГОСТ Р34.10-94

Вариант 2.

1. Построить систему Эль-Гамала $p=7$, $q=13$
2. Построить систему Рабина
3. Привести пример системы доказательства с нулевым знанием
4. Схема ЭЦП DSA.

Вопросы для подготовки к зачету.

- 1 Понятие математической защиты информации и информационной безопасности
- 2 Способы защиты информации.
- 3 Некоторые исторические алгоритмы (алгоритмы Цезаря, Вижнера).
- 4 Криптоанализ исторических алгоритмов (алгоритмы Цезаря, Вижнера).
- 5 Влияние длины блока на криптографическую стойкость алгоритма (алгоритмы Хилла и Пифнера).
- 6 Сравнение классических одноалфавитных и многоалфавитных систем.
- 7 Идея открытых ключей и преимущества их.
- 8 Рюкзачная криптосистема.
- 9 Криптоанализ рюкзачной криптосистемы.
- 10 Плотный рюкзак.
- 11 Криптосистема RSA.
- 12 Криптоанализ криптосистемы RSA.
- 13 Криптосистемы основанные на дискретных логарифмах.
- 14 Криптосистема Рабина.
- 15 Криптосистема Уильямса.
- 16 Криптосистема Эль-Гамеля.
- 17 Криптосистема Вильямса.
- 18 Способы передачи ключей.
- 19 Криптосистемы основанные на эллиптических кривых.
- 20 Обзор потоковых кодов.
21. Симметричные криптосистемы
22. Доказательство с нулевым знанием
23. ЭЦП
24. Разделение секрета. Подсознательный канал