МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра дифференциальных уравнений

УТВЕРЖДАЮ
Декан математического факультета

Нестеров П.Н.
20 июня 2023 г.

Рабочая программа дисциплины

Компьютерная безопасность

Направление подготовки (специальности)
01.03.02 Прикладная математика и информатика

Направленность (профиль)
«Прикладное программирование и информационные технологии»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 19 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Дисциплина «Компьютерная безопасность» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию практических навыков конструирования систем защиты информации, а также особенностей применения криптографических методов в более общих ситуациях.

Задача дисциплины – дать основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов.

Практические занятия проводятся в учебных группах и имеют целью закрепление теоретических основ дисциплины, излагаемых в лекционном курсе.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Компьютерная безопасность» расположена на стыке теоретической и прикладной математики и основывается на знаниях, полученных слушателями при изучении дисциплин «Алгебра и геометрия», «Численные методы» и «Основы программирования». Знания и навыки, полученные при изучении дисциплины, используются при написании курсовых проектов и выпускных работ.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности.

Код компетенции	Формулировка компетенции	Перечень планируемых результатов Обучения
ПК-2	способностью понимать, совершенствовать и применять современный математический аппарат	**иметь представление:** • о применении криптографии в решении задач аутентификации, построения систем цифровой подписи; • о государственных стандартах в области криптографии; • о методах криптозащиты компьютерных систем и сетей **владеть:** • современной научно-технической литературы в области криптографической защиты.

		владеть: • навыками использования основных криптографических протоколов; **знать и уметь использовать:** • типовые криптографические протоколы; • протоколы управления ключами; основные методы, используемые в построении протоколов

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет __ зачетные единицы, __ акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)* Формы ЭО и ДОТ *(при наличии)*
			Контактная работа						
			лекции	Практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1.1	**Традиционные бумажные и электронные документы.** Документ на бумажном носителе и рукописная подписью Электронные документы. Угрозы безопасности субъектам электронного документооборота.		2					4	
	в том числе с ЭО и ДОТ							*2*	
1.2	**Криптографические методы защиты информации.** Криптография с симметричными ключами. Криптография с открытыми ключами. Доверие к открытому ключу и цифровые сертификаты.		4	2				4	
	в том числе с ЭО и ДОТ							*2*	

1.3	**Криптографические методы защиты информации.** Кольцо и поле вычетов. Решение простейших уравнений в Z(m).								
	в том числе с ЭО и ДОТ								
1.4	**Криптографическиее методы защиты информации.** Алгоритм Эвклида и его реализации.								Выполнение практической работы №1
	в том числе с ЭО и ДОТ								
1.5	**Криптографическиее методы защиты информации.** Последовательность Фибоначи и ее свойства. Оценки роста								
	в том числе с ЭО и ДОТ								
1.6	**Криптографическиее методы защиты информации.** Оценки сложности алгоритмов. Оценка сложности вычисления НОД.								
	в том числе с ЭО и ДОТ								
1.7	**Криптографическиее методы защиты информации.** Криптосистемы с линейной функцией в Z(m). Взлом линейных систем за полиномиальное число операций.								
	в том числе с ЭО и ДОТ								
1.8	**Криптографическиее методы защиты информации.** Решение диофантовых уравнений. Оценка сложности.								Выполнение практической работы №2
	в том числе с ЭО и ДОТ								
1.9	**Криптографическиее методы защиты информации.** Функция Эйлера и ее свойства.								
	в том числе с ЭО и ДОТ								

1.10	**Криптографическиее методы защиты информации.** Теоремы Ферма и Эйлера								
	в том числе с ЭО и ДОТ								
1.11	**Криптографические методы защиты информации.** Решение степенных уравнений в Z(m). Оценки сложности								Выполнение контрольной работы №1
	в том числе с ЭО и ДОТ								
2.1	**Модели криптографических протоколов.** Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Требования к криптографическому протоколу.		4	2				4	Подготовка докладов для семинарского занятия
	в том числе с ЭО и ДОТ								
2.2	**Цифровая подпись.** Протоколы цифровых подписей RSA, Эль-Гамаля, с посредником. Стандарты цифровой подписи DSS и Р34. Протокол электронной подписи Шнорра.		4					4	Подготовка докладов для семинарского занятия
	в том числе с ЭО и ДОТ								
2.3	Реализация схем электронной подписи на ЭВМ.			2				4	Выполнение практической работы №3
	в том числе с ЭО и ДОТ								
2.4	**Методы хэширования.** Стандарты MD-4, MD-5. Анализ некоторых алгоритмов выработки хэш-функций.		4	2				4	Подготовка докладов для семинарского занятия
	в том числе с ЭО и ДОТ								
2.5	**Протоколы аутентификации и идентификации.** Протоколы «рукопожатия», Окамото. Взаимосвязь между протоколами аутентификации и цифровой подписи.		2					4	Подготовка докладов для семинарского занятия
	в том числе с ЭО и ДОТ								

2.6	**Протоколы голосования.** Протоколы Шаума и Педерсена. Разделение секрета. Протоколы конфиденциального вычисления.		2					4	Подготовка докладов для семинарского занятия
	в том числе с ЭО и ДОТ								
2.7	**Протоколы управления ключами.** Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации. Протокол Керберос.		4					4	Подготовка докладов для семинарского занятия
	в том числе с ЭО и ДОТ								
2.8	Построение криптографического протокола распределения ключей. Анализ некоторых схем открытого распределения ключей.			2				2	Выполнение практической работы №3
	в том числе с ЭО и ДОТ								
2.9	**Особенности реализации криптосистем.** Проблема реализации криптографической подсистемы и системы управления ключами. Криптографические интересы GSS-API, DASS. Системы TSS, PGP, PEM. Электронные деньги. Протоколы SET. Рекомендации X509.		2	2				4	
	в том числе с ЭО и ДОТ								
2.10	**Другое применение криптографии.** Доказательства с нулевым разглашением. Разделение секрета. Протоколы типа подбрасывания монеты. Протоколы игры в покер. Идеальное разделение секрета и матроиды.		2	2				4	
	в том числе с ЭО и ДОТ							*2*	
2.11	**Правовые вопросы применения электронного документооборота в Рос-**		4					2	

	сии. Особенности юридического определения электронного документооборота. Закон РФ «Об электронной цифровой подписи». Цель принятия и сфера действия закона. Соотношение между аналогом собственноручной подписи, цифровой подписью и ЭЦП. Что такое ЭЦП в соответствии с законом.								
	в том числе с ЭО и ДОТ								
	ИТОГО								
	в том числе с ЭО и ДОТ								

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

Активные и интерактивные формы проведения занятий.

При реализации различных видов учебной работы используются образовательные технологии, направленные на развитие у студентов творческих способностей и самостоятельности.

Практические занятия как форма обучения позволяют более полно реализовать компетентностный подход во взаимодействии с контекстным, проблемным и личностно-ориентированным подходами с опорой на интерактивные методы обучения, которые основаны на принципах взаимодействия студентов друг с другом, активности, опоре на групповой опыт при обязательной обратной связи. На практических занятиях в процессе целесообразно использовать следующие интерактивные методы: метод кейсов, деловые игры, мозговой штурм, дебаты. Использование данных интерактивных методов позволит:

- более эффективно организовать учебный процесс, сочетая традиционное обучение с новыми современными технологиями;
- повысить мотивацию студентов к получению знаний;
- формировать ценностное отношения к будущей педагогической деятельности, так как с помощью интерактивных методов студент вовлекается в моделируемую преподавателем будущую профессиональную деятельность;
- повысить уровень сформированности ключевых профессиональных компетенций и личностных качеств.

Курс обучения предполагает чтение научной литературы отечественных и

зарубежных авторов, использование интернет-ресурсов.

В процессе обучения используются следующие технологии электронного обучения и дистанционные образовательные технологии:

Электронный учебный курс «Компьютерная безопасность» в LMS Электронный университет Moodle ЯрГУ, в котором:

- представлены задания для самостоятельной работы обучающихся при подготовке к экзамену;
- осуществляется проведение отдельных мероприятий текущего контроля успеваемости студентов;
- презентации и видео лекций по темам дисциплины;
- представлены правила прохождения промежуточной аттестации по дисциплине;
- посредством форума и системы сообщений осуществляется синхронное и (или) асинхронное взаимодействие между обучающимися и преподавателем в рамках изучения дисциплины.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса используются:

– для формирования текстов материалов для промежуточной и текущей аттестации – программы Microsoft Office, издательская система LaTex;

– для поиска учебной литературы библиотеки ЯрГУ – Автоматизированная библиотечная информационная система «БУКИ-NEXT» (АБИС «Буки-Next»).

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная учебная литература:

1. А.А. Стрельцов Обеспечение информационной безопасности России. Теоретические и методологические основы. М., МЦНМО, 2002

2. А.В. Черемушкин Лекции по арифметическим алгоритмам в криптографии. М., МЦНМО, 2002

3. А.Ю. Зубов Крипографические методы защиты информации. Совершенные шифры: учебное пособие для вузов. М., Гелиос АРВ, 2005. – 191с..

4. В.А. Пярин, А.С. Кузьмин, С.Н. Смирнов Безопасность электронного бизнеса. М., Гелиос АРВ, 2003
5. В.М. Сидельников Криптография и теория кодирования.
6. С.Г. Баричев, Р.Е. Серов Основы современной криптографии. М.: Горячая линия - Телеком, 2002
7. Э.А. Применко, А.А Грушо Е.Е. Тимонина Анализ и синтез криптоалгоритмов. Курс лекций. М, 2000

б) дополнительная учебная литература:

8. О.А. Логачев, А.А. Сальников, В.В. Ященко Криптографические свойства дискретных функций. Материалы конференции «Московский университет и развитие криптографии в России», МГУ, 17-18 октября 2002
9. О.Н. Василенко Теоретико-числовые алгоритмы в криптографии. М., МЦНМО, 2003

в) ресурсы сети «Интернет»

10. Электронные каталоги НБ ЯрГУ - http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php
11. Электронная библиотека учебных материалов ЯрГУ - http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php
12. Электронный архив ЯрГУ - http://elar.uniyar.ac.ru/jspui/community-list
13. http://www.cryptography.ru
14. http://algolist.manual.ru/defence/intro.php
15. http://algo.4u.ru

Ресурсы в свободном доступе.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

-учебные аудитории для проведения занятий лекционного типа и практических занятий (семинаров);

- учебные аудитории для проведения групповых и индивидуальных консультаций,

- учебные аудитории для проведения текущего контроля и промежуточной аттестации;

-помещения для самостоятельной работы;

-помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ЯрГУ.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Составитель:

Д.ф.-м.н., профессор _____ Бережной Е.И.

Приложение №1 к рабочей программе дисциплины
«Компьютерная безопасность»

Фонд оценочных средств для проведения текущей и промежуточной аттестации студентов по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1. Контрольные задания и иные материалы, используемые в процессе текущей аттестации

Примерные варианты контрольных работ:

Контрольная работа № 1

1. Сколько решений имеет уравнение x^2 = xmod(m) в зависимости от числа делителей m?

2. Найти последнюю цифру числа

33^222 в восьмеричной системе

33^222 в девятеричной системе

33^222 в десятичной системе

3.Найти все решения уравнения ax + by = c

a=7, b=22, c=3;

a=9, b=25, c=3;

a=13 b=25, c=1.

5. Зашифруйте слово «ДЕКАНАТ» шифром Цезаря.

6. Какой метод криптоанализа наиболее эффективен для взлома шифра Цезаря?

а) Анализ с избранным текстом;

б) Анализ с избранным зашифрованным текстом;

в) Анализ с избранным открытым текстом;

г) Анализ с известным открытым текстом

д) Анализ только шифрованного текста.

7. Что такое симметричное шифрование?

а) способ шифрования, при котором каждый символ (или последовательность символов) исходного сообщения заменяются другим символом (или другой последовательностью символов);

б) способ шифрования, при котором один и тот же ключ используется и для шифрования и для расшифрования текста;

в) способ шифрования, при котором используются два свзяанных ключа: один для

шифрования, другой для расшифрования;

г) способ шифрования, при котором символы открытого текста изменяют порядок

следования в соответствии с правилом, которое определяется ключом.

8. В чем заключается основная проблема использования симметричных алгоритмов?

а) Сложность реализации на ЭВМ;

б) Легкость криптоанализа таких шифров с появлением ЭВМ;

в) Трудности при передаче ключей и управлении ими;

г) Работа этих алгоритмов на ЭВМ требует значительных вычислительных ресурсов.

Контрольная работа № 2

1. Чтобы подписать сообщение электронной цифровой подписью, используются:

а) открытый ключ отправителя;

б) открытый ключ получателя;

в) закрытый ключ отправителя;

г) закрытый ключ получателя.

2. Какие утверждения о протоколе строгой двусторонней аутентификации на основе

случайных чисел справедливы?

а) в основе протокола лежит симметричный алгоритм шифрования;

б) на первом шаге проверяющий В отправляет проверяемому А случайное число;

в) на втором шаге проверяемый А отправляет проверяющему В зашифрованное сообщение, содержащее полученное на первом шаге случайное число, а также новое случайное число.

г) всего протокол требует отправки двух сообщений.

3. Какова последовательность подписания сообщений с помощью ЭЦП?

а) вычисляется хэш, затем хэш зашифровывается;

б) сообщение зашифровывается, после чего результат хэшируется;

в) при подписании сообщение зашифровывается, при проверке вычисляется хэш;

г) вычисляется хэш исходного сообщения, после чего оно зашифровывается.

4. В чем заключается такое свойство функции хэширования H как стойкость к коллизиям первого рода?

а) Для любого хэша h должно быть практически невозможно вычислить или подобрать такое x, что H(x) = h.

б) Должно быть практически невозможно вычислить или подобрать любую пару

различных сообщений x и y для которых H(x) = H(y);

в) Длина хэша должна быть фиксированной независимо от длины входного сообщения;

г) Для любого сообщения x должно быть практически невозможно вычислить или

подобрать другое сообщение y, такое что H(x) = H(y).

5. Доказательство корректности алгоритма RSA основано на:

а) теореме Эйлера;

б) теореме о сумме эллиптических кривых;

в) китайской теореме об остатках;

г) расширенном алгоритме Евклида.

6. Какими свойствами должен обладать генератор псевдослучайных чисел?

а) недетерминированность;

б) непредсказуемость;

в) независимость очередного элемента от предыдущего;

г) равномерное распределение элементов последовательности;

д) неповторяемость элементов последовательности (в пределах периода).

7. Какие из перечисленных алгоритмов являются алгоритмами электронной цифровой подписи?

а) DES;

б) ГОСТ Р 34.10—2001;

в) ГОСТ Р 34.11—94;

г) RSA.

8. Открытым ключом RSA является пара (15, 2). Зашифруйте число 4.

9. Эллиптическая кривая имеет вид:

а) $y2 = x3 + ax + b \pmod p$;

б) $y3 = x2 + ax + b \pmod p$;

в) $y = x3 + ax2 + b \pmod p$;

г) $x3 = y2 + ax + b \pmod p$.

10. Чтобы расшифровать сообщение с помощью асимметричного алго-

ритма шифрования используются:

а) открытый ключ отправителя;

б) открытый ключ получателя;

в) закрытый ключ отправителя;

г) закрытый ключ получателя.

Примерные темы для семинарских занятий

Протоколы аутентификации. Схема Эль Гамаля.

Протоколы аутентификации. Схема Шнорра.

Алгоритм Диффи-Хеллмана

Алгоритм RSA

ЭЦП Эль Гамаля

ЭЦП Шнорра

Эллиптические кривые над конечным полем.

ЭЦП с использованием эллитических кривых.

Функции хеширования и их свойства.

Протоколы раздачи карт без карт.

Протоколы голосования.

Протоколы подбрасывания монет.

Примеры заданий для практических (лабораторных) работ

1. Используя любой язык программирования, напишите программу, реализующую соответствующий алгоритм шифрования/дешифрования (варианты распределяются преподавателем):

Модифицированный шифр Цезаря (ключом является любое число).

Моноалфавитный шифр (шифр простой замены).

Простой перестановочный шифр.

Решетка Флейберга.

Скремблер.

2. Напишите программу, реализующую ЭЦП:

Эль Гамаля.

Шнорра.

ЭЦП с использованием эллитических кривых.

3. Напишите реализацию MD-4, MD-5

4. Напишите реализацию протокола подбрасывания монеты.

5. Напишите реализацию протокола игры в покер для 2, 3, 4 игроков.

6. Напишите реализацию протокола распределения ключей Cerberos.

7. Напишите реализацию протокола распределения ключей Диффи – Хеллмана.

8. Напишите реализацию алгоритма проверки числа на простоту.

1.2. Список вопросов и (или) заданий для проведения промежуточной аттестации

1. Кольцо и поле вычетов. Свойства и примеры.
2. Кольцо и поле вычетов. Решение линейных уравнений в Z(m).
3. Кольцо и поле вычетов. Решение квадратных уравнений в Z(m).
4. Алгоритм Эвклида.
5. Уравнение Фиббоначи. Структура решений.
6. Уравнение Фиббоначи. Оценки роста фундаментальных решений.
7. Сложность алгоритмов
8. Оценки сложности алгоритма Эвклида.
9. Решение диофантовых уравнений от двух переменных. Теоремы существования и структура решений.
10. Решение диофантовых уравнений от двух переменных. Оценки сложности.
11. Решение диофантовых уравнений от n-переменных. Оценки сложности.
12. Функция Эйлера и ее вычисление.
13. Теорема Ферма.
14. Теорема Эйлера.
15. Решение уравнений x^n mod(m) =a. Теоремы существования.
16. Решение уравнений x^n mod(m) =a. Оценки сложности.

2. Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

2.1 Шкала оценивания сформированности компетенций и ее описание

Оценивание уровня сформированности компетенций в процессе освоения дисциплины осуществляется по следующей трехуровневой шкале:

Пороговый уровень - предполагает отражение тех ожидаемых результатов, которые определяют минимальный набор знаний и (или) умений и (или) навыков, полученных студентом в результате освоения дисциплины. Пороговый уровень является обязательным уровнем для студента к моменту завершения им освоения данной дисциплины.

Продвинутый уровень - предполагает способность студента использовать знания, умения, навыки и (или) опыт деятельности, полученные при освоении дисциплины, для решения профессиональных задач. Продвинутый уровень превосходит пороговый уровень по нескольким существенным признакам.

Высокий уровень - предполагает способность студента использовать потенциал интегрированных знаний, умений, навыков и (или) опыта деятельности, полученных при освоении дисциплины, для творческого решения профес-

сиональных задач и самостоятельного поиска новых подходов в их решении путем комбинирования и использования известных способов решения применительно к конкретным условиям. Высокий уровень превосходит пороговый уровень по всем существенным признакам.

2.2 Перечень компетенций, этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования

Код компетенции	**Форма контроля**	**Этапы формирования (№ темы, раздела)**	**Показатели оценивания**	**Шкала и критерии оценивания компетенций на различных этапах их формирования**		
				Пороговый уровень	**Продвинутый уровень**	**Высокий уровень**
ПК-2	семинары, практические работы	все	иметь представление	о применении криптографии в решении задач аутентификации, построения систем цифровой подписи	о применении криптографии в решении задач аутентификации, построения систем цифровой подписи	о применении криптографии в решении задач аутентификации, построения систем цифровой подписи
				о методах криптозащиты компьютерных систем и сетей	о методах криптозащиты компьютерных систем и сетей	о методах криптозащиты компьютерных систем и сетей
					о государственных стандартах в области криптографии	о государственных стандартах в области криптографии
			владеть			знаниями современной научно-технической литературы в области криптографической защиты
	семинары, КР, практические работы	все	владеть	навыками использования основных криптографических протоколов	навыками использования основных криптографических протоколов	навыками использования основных криптографических протоколов
			знать	типовые криптографические протоколы	типовые криптографические протоколы	типовые криптографические протоколы
			знать и уметь использовать		основные методы, используемые в построении протоколов	основные методы, используемые в построении протоколов
						протоколы управления ключами

3. Методические рекомендации преподавателю по процедуре оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Целью процедуры оценивания является определение степени овладения студентом ожидаемыми результатами обучения (знаниями, умениями, навыками и (или) опытом деятельности).

Процедура оценивания степени овладения студентом ожидаемыми результатами обучения осуществляется с помощью методических материалов, представленных в разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций»

3.1 Критерии оценивания степени овладения знаниями, умениями, навыками и (или) опытом деятельности, определяющие уровни сформированности компетенций

Пороговый уровень (общие характеристики):

- владение основным объемом знаний по программе дисциплины;
- знание основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы без существенных ошибок;
- владение инструментарием дисциплины, умение его использовать в решении стандартных (типовых) задач;
- способность самостоятельно применять типовые решения в рамках рабочей программы дисциплины;
- усвоение основной литературы, рекомендованной рабочей программой дисциплины;
- знание базовых теорий, концепций и направлений по изучаемой дисциплине;
- самостоятельная работа на практических и лабораторных занятиях, периодическое участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

Продвинутый уровень (общие характеристики):

- достаточно полные и систематизированные знания в объёме программы дисциплины;
- использование основной терминологии данной области знаний, стилистически грамотное, логически правильное изложение ответа на вопросы,

умение делать выводы;

- владение инструментарием дисциплины, умение его использовать в решении учебных и профессиональных задач;
- способность самостоятельно решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- усвоение основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;
- самостоятельная работа на практических и лабораторных занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Высокий уровень (общие характеристики):

- систематизированные, глубокие и полные знания по всем разделам дисциплины;
- точное использование терминологии данной области знаний, стилистически грамотное, логически верное изложение ответа на вопросы, умение делать обоснованные выводы;
- безупречное владение инструментарием дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;
- способность самостоятельно и творчески решать сложные задачи (проблемы) в рамках рабочей программы дисциплины;
- глубокое усвоение необходимого материала из основной и дополнительной литературы, рекомендованной рабочей программой дисциплины;
- умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой дисциплине и давать им критическую оценку;
- активная самостоятельная работа на практических и лабораторных занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

3.2 Описание процедуры выставления оценки

В зависимости от уровня сформированности каждой компетенции по окончании освоения дисциплины студенту выставляется оценка. Для дисциплин, изучаемых в течение нескольких семестров, оценка может выставляться не только по окончании ее освоения, но и в промежуточных семестрах. Вид оценки («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»,

«зачтено», «не зачтено») определяется рабочей программой дисциплины в соответствии с учебным планом.

Оценка «отлично» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована на высоком уровне.

Оценка «хорошо» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на продвинутом уровне.

Оценка «удовлетворительно» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «неудовлетворительно» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Оценка «зачтено» выставляется студенту, у которого каждая компетенция (полностью или частично формируемая данной дисциплиной) сформирована не ниже, чем на пороговом уровне.

Оценка «не зачтено» выставляется студенту, у которого хотя бы одна компетенция (полностью или частично формируемая данной дисциплиной) сформирована ниже, чем на пороговом уровне.

Приложение №2 к рабочей программе дисциплины
«Компьютерная безопасность»

Методические указания для студентов по освоению дисциплины

Студенту желательно проявлять активное участие на занятиях, задавать вопросы, поскольку умение обосновывать свою точку зрения, нахождение компромиссного решения в этически выдержанной дискуссии не только важно для лучшего усвоения материала, но и ценится в реальной жизни. Важным моментом при изучении любой дисциплины является организация самостоятельной работы.

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов в ВУЗе является важным видом учебной и научной деятельности студента. Государственным стандартом предусматривается, как правило, 50% часов из общей трудоемкости дисциплины на самостоятельную работу студентов (далее СРС). В связи с этим, обучение в ВУЗе включает в себя две, практически одинаковые по объему и взаимовлиянию части – процесса обучения и процесса самообучения. Поэтому СРС должна стать эффективной и целенаправленной работой студента.

Концепцией модернизации российского образования определены основные задачи профессионального образования - «подготовка квалифицированного работника соответствующего уровня и профиля, конкурентоспособного на рынке труда, компетентного, ответственного, свободно владеющего своей профессией и ориентированного в смежных областях деятельности, способного к эффективной работе по специальности на уровне мировых стандартов, готового к постоянному профессиональному росту, социальной и профессиональной мобильности».

Решение этих задач невозможно без повышения роли самостоятельной работы студентов над учебным материалом, усиления ответственности преподавателей за развитие навыков самостоятельной работы, за стимулирование профессионального роста студентов, воспитание творческой активности и инициативы.

Формирование такого умения происходит в течение всего периода обучения через участие студентов в практических занятиях, выполнение контроль-

ных заданий и тестов, написание курсовых и выпускных квалификационных работ. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

В освоении дисциплины (модуля) инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации по предмету является важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

Для самостоятельной работы особенно рекомендуется использовать следующую учебную литературу:

1. А.А. Стрельцов Обеспечение информационной безопасности России. Теоретические и методологические основы. М., МЦНМО, 2002
2. А.В. Черемушкин Лекции по арифметическим алгоритмам в криптографии. М., МЦНМО, 2002
3. А.Ю. Зубов Совершенные шифры. Дополнительные главы курса криптографии. М., Гелиос АРВ, 2003
4. В.А. Пярин, А.С. Кузьмин, С.Н. Смирнов Безопасность электронного бизнеса. М., Гелиос АРВ, 2003
5. В.М. Сидельников Криптография и теория кодирования.

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

1. 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.).

2. 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. Головной 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 стандартизованной форме метаданные внешних ресурсов, а также содержит описания полнотекстовых публикаций электронной библиотеки. Общий объем каталога превышает 56 000 мета-описаний (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.

Для самостоятельного подбора литературы в библиотеке ЯрГУ рекомендуется использовать:

1. Личный кабинет (http://lib.uniyar.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.uniyar.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.uniyar.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.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.