

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

Кафедра дифференциальных уравнений

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

21 мая 2024 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 2024 г., протокол № 8

Программа одобрена НМК  
математического факультета  
протокол № 9 от 3 мая 2024 г.

## 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

Данная дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, и является элективной дисциплиной. 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.

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
<b>Профессиональные компетенции</b>		
<b>ПК-2</b> Способен понимать, совершенствовать и применять современный математический аппарат	<b>И-ПК-2.1</b> Обладает устойчивыми знаниями в области основных математических дисциплин, их аппарата и результатов <b>И-ПК-2.2</b> Обладает способностью применять современный математический аппарат в решении различных задач <b>И-ПК-2.3</b> Способен совершенствовать свои навыки, связанные с применением современного математического аппарата	<b>Знать:</b> - типовые криптографические протоколы; - протоколы управления ключами; - основные методы, используемые в построении протоколов; - о государственных стандартах в области криптографии; - о методах криптозащиты компьютерных систем и сетей <b>Владеть навыками:</b> - применения криптографии в решении задач аутентификации, построения систем цифровой подписи; - использования основных криптографических протоколов; - использования современной научно-технической литературы в области криптографической защиты.

#### 4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **4** зачетные единицы, **144** акад. часа.

№ 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)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Традиционные бумажные и электронные документы	7	1	1				3	
2	Криптографические методы защиты информации. Криптография с симметричными ключами. Криптография с открытыми ключами. Доверие к открытому ключу и цифровые сертификаты	7	1	1				3	
3	Кольцо и поле вычетов. Решение простейших уравнений в $Z(m)$	7	2	1				3	
4	Алгоритм Эвклида и его реализации	7	1	3		2		3	Выполнение практической работы №1
5	Последовательность Фиббоначи и ее свойства. Оценки роста	7	1	1				3	
6	Оценки сложности алгоритмов. Оценка сложности вычисления НОД	7	2	1				3	
7	Криптосистемы с линейной функцией в $Z(m)$ . Взлом линейных систем за полиномиальное число операций	7	2	1				3	
8	Решение диофантовых уравнений. Оценка сложности.	7	1	3		2		3	Выполнение практической работы №2
9	Функция Эйлера и ее свойства.	7	2	1				3	
10	Теоремы Ферма и Эйлера	7	1	1				3	
11	Решение степенных уравнений в $Z(m)$ . Оценки	7	2	2				3	Выполнение контрольной работы №1

	сложности								
							<b>0,3</b>	<b>2,7</b>	<b>Зачет</b>
	<b>Всего за 7 семестр 72 акад. часа</b>		<b>16</b>	<b>16</b>		<b>4</b>	<b>0,3</b>	<b>35,7</b>	
12	Модели криптографических протоколов	8		2				2	Подготовка докладов для семинарского занятия
13	Цифровая подпись	8		1				2	Подготовка докладов для семинарского занятия
14	Реализация схем электронной подписи на ЭВМ	8		3		1		1	Выполнение практической работы №3
15	Методы хэширования	8		1				2	Подготовка докладов для семинарского занятия
16	Протоколы аутентификации и идентификации	8		1				2	Подготовка докладов для семинарского занятия
17	Протоколы голосования	8		1				2	Подготовка докладов для семинарского занятия
18	Протоколы управления ключами	8		1				2	Подготовка докладов для семинарского занятия
19	Построение криптографического протокола распределения ключей. Анализ некоторых схем открытого распределения ключей.	8		3		1		1	Выполнение практической работы №4
20	Особенности реализации криптосистем.	8		1				1	
21	Другое применение криптографии.	8		1				1	
22	Правовые вопросы применения электронного документооборота в России	8		1				2	
						<b>2</b>	<b>0,5</b>	<b>33,5</b>	<b>Экзамен</b>
	<b>Всего за 8 семестр 72 акад. часа</b>			<b>16</b>		<b>4</b>	<b>0,5</b>	<b>51,5</b>	
	<b>ИТОГО</b>		<b>16</b>	<b>32</b>		<b>8</b>	<b>0,8</b>	<b>87,2</b>	

#### Содержание разделов дисциплины:

##### Тема 1. Традиционные бумажные и электронные документы.

Документ на бумажном носителе и рукописная подписью Электронные документы. Угрозы безопасности субъектам электронного документооборота.

**Тема 2. Криптографические методы защиты информации. Криптография с симметричными ключами. Криптография с открытыми ключами. Доверие к открытому ключу и цифровые сертификаты.**

**Тема 3. Кольцо и поле вычетов. Решение простейших уравнений в  $Z(m)$ .**

**Тема 4. Алгоритм Эвклида и его реализации.**

**Тема 5. Последовательность Фибоначчи и ее свойства. Оценки роста**

**Тема 6. Оценки сложности алгоритмов. Оценка сложности вычисления НОД.**

**Тема 7. Криптосистемы с линейной функцией в  $Z(m)$ . Взлом линейных систем за полиномиальное число операций.**

**Тема 8. Решение диофантовых уравнений. Оценка сложности.**

**Тема 9. Функция Эйлера и ее свойства.**

**Тема 10. Теоремы Ферма и Эйлера**

**Тема 11. Решение степенных уравнений в  $Z(m)$ . Оценки сложности**

**Тема 12. Модели криптографических протоколов.**

Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Требования к криптографическому протоколу.

**Тема 13. Цифровая подпись.**

Протоколы цифровых подписей RSA, Эль-Гамала, с посредником. Стандарты цифровой подписи DSS и P34. Протокол электронной подписи Шнорра.

**Тема 14. Реализация схем электронной подписи на ЭВМ.**

**Тема 15. Методы хэширования.**

Стандарты MD-4, MD-5. Анализ некоторых алгоритмов выработки хэш-функций.

**Тема 16. Протоколы аутентификации и идентификации.**

Протоколы «рукопожатия», Окамото. Взаимосвязь между протоколами аутентификации и цифровой подписи.

**Тема 17. Протоколы голосования.**

Протоколы Шаума и Педерсена. Разделение секрета. Протоколы конфиденциального вычисления.

**Тема 18. Протоколы управления ключами.**

Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификации. Протокол Керберос.

**Тема 19. Построение криптографического протокола распределения ключей. Анализ некоторых схем открытого распределения ключей.**

**Тема 20. 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.

**Тема 21. Другое применение криптографии.**

Доказательства с нулевым разглашением. Разделение секрета. Протоколы типа подбрасывания монеты. Протоколы игры в покер. Идеальное разделение секрета и матроиды.

**Тема 22. Правовые вопросы применения электронного документооборота в России.**

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.

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

В процессе обучения используются следующие образовательные технологии:

**Академическая лекция с элементами лекции-беседы** – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя.

Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

**Практическое занятие** – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

**Консультации** – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

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

В процессе осуществления образовательного процесса по дисциплине используются: для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTeX;
- Adobe Acrobat Reader.

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

В процессе осуществления образовательного процесса по дисциплине используются:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»

[http://www.lib.uniyar.ac.ru/opac/bk\\_cat\\_find.php](http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php)

- Электронная библиотечная система «Лань» <https://e.lanbook.com>

- Электронная библиотечная система «Юрайт» <https://urait.ru>

- Электронная библиотечная система «Консультант студента»  
<https://www.studentlibrary.ru>

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

### **а) основная литература**

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

<https://library.tsilikin.ru/Естественные%20науки/Математика/Черемушкин%20А.В.%20Лекции%20по%20арифметическим%20алгоритмам%20в%20криптографии.pdf>

2. А. Ю. Зубов Криптографические методы защиты информации. Совершенные шифры: учебное пособие для вузов. - М., Гелиос АРВ, 2005.

3. Сидельников В. М. Теория кодирования. - Москва: ФИЗМАТЛИТ, 2008.

<https://www.studentlibrary.ru/ru/book/ISBN9785922109437.html>

4. С. Г. Баричев, Р. Е. Серов Основы современной криптографии. - М.: Горячая линия

- Телеком, 2002 [http://lib.ysu.am/open\\_books/417394.pdf](http://lib.ysu.am/open_books/417394.pdf)

5. Э. А. Применко, А. А. Грушо Е. Е. Тимонина Анализ и синтез криптоалгоритмов. Курс лекций. – М.:, 2000

<https://istina.msu.ru/publications/book/11098328/?ysclid=ln1q1o26r0501119689>

**б) дополнительная литература**

1. 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 [http://www.iisi.msu.ru/UserFiles/File/publications/mos\\_univ\\_crypt.pdf](http://www.iisi.msu.ru/UserFiles/File/publications/mos_univ_crypt.pdf)

2. О. Н. Василенко Теоретико-числовые алгоритмы в криптографии. - М., МЦНМО, 2006 <https://djvu.online/file/sNt61WMCyNUMV?ysclid=ln1pt8zllly567263292>

3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2023. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/511239>

4. В. А. Пярин, А. С. Кузьмин, С. Н. Смирнов Безопасность электронного бизнеса. - М., Гелиос АРВ, 2003

**в) ресурсы сети «Интернет»**

1. Алгоритмы, методы, исходники: <http://algotlist.manual.ru/defence/intro.php>

**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;
- учебные аудитории для проведения 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 к электронной информационно-образовательной среде ЯрГУ.

**Автор:**

Д.ф.-м.н., профессор

Бережной Е. И.

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

**1. Типовые контрольные задания или иные материалы,  
используемые в процессе текущей аттестации**

Примерные варианты контрольных работ:

**Контрольная работа № 1**

1. Сколько решений имеет уравнение  $x^2 = x \bmod(m)$  в зависимости от числа делителей  $m$ ?
2. Найти последнюю цифру числа  $33^{222}$  в восьмеричной системе
3.  $33^{222}$  в девятеричной системе
3.  $33^{222}$  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 связанных 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)  $y^2 = x^3 + ax + b \pmod{p}$ ;
  - б)  $y^3 = x^2 + ax + b \pmod{p}$ ;
  - в)  $y = x^3 + ax^2 + b \pmod{p}$ ;
  - г)  $x^3 = y^2 + ax + b \pmod{p}$ .
10. Чтобы расшифровать сообщение с помощью асимметричного алгоритма 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 Гамала.

Протоколы аутентификации. Схема Шнорра.

Алгоритм Диффи-Хеллмана

Алгоритм RSA

ЭЦП Эль Гамала

ЭЦП Шнорра

Эллиптические кривые над конечным полем.

ЭЦП с использованием эллиптических 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 Гамала.

Шнорра.

ЭЦП с использованием эллиптических 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.

**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  $x^n \bmod(m) = a$ . Теоремы существования.
16. Решение уравнений  $x^n \bmod(m) = a$ . Оценки сложности.

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

#### 3.1 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 профессиональных 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.

#### 3.2 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, практич	все	владеть	навыками использования основных	навыками использования основных	навыками использования основных криптографических

	еские работы			криптографических протоколов	криптографических протоколов	протоколов
			знать	типовые криптографические протоколы	типовые криптографические протоколы	типовые криптографические протоколы
			знать и уметь использо вать		основные методы, используемые в построении протоколов	основные методы, используемые в построении протоколов
						протоколы управления ключами

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»

### **3.3. 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 объеме 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.

### **3.4 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.

**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 контрольных 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.