




МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
федеральное государственное автономное образовательное учреждение высшего образования  
**«Дальневосточный федеральный университет»**  
(ДФУ)

**ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)**

СОГЛАСОВАНО  
Руководитель ОП

  
(подпись) Гузев М.А.  
(ФИО)

**«УТВЕРЖДАЮ»**  
Директор департамента  
  
(подпись) Сущенко А.А.  
(ФИО)  
« 25 » марта 2022 г.



**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**  
**Технологии защиты информации**  
**Направление подготовки 09.03.03 Прикладная информатика**  
**(Прикладная информатика в компьютерном дизайне)**  
**Форма подготовки очная**

курс 3 семестр 6  
лекции 18 час.  
практические занятия час.  
лабораторные работы час.  
в том числе с использованием МАО лек. / пр., лаб.  
всего часов аудиторной нагрузки час.  
в том числе с использованием МАО  
самостоятельная работа 18 час.  
в том числе на подготовку к экзамену час.  
контрольные работы (количество)  
курсовая работа/курсовой проект семестр  
зачет 6 семестры  
экзамен семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта по направлению подготовки 09.03.03 Прикладная информатика утвержденного приказом Министерства образования и науки РФ от 19 сентября 2017 г. № 922 (с изменениями и дополнениями).

Рабочая программа обсуждена на заседании департамента математического и компьютерного моделирования протокол №10 от « 25 » марта 2022г.

Директор департамента математического и компьютерного моделирования Сущенко А.А.  
Составители: ст.преподаватель Серга И.В.

Владивосток  
2022

**Оборотная сторона титульного листа РПД**

**I. Рабочая программа пересмотрена на заседании департамента:**

Протокол от «\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_

Директор департамента \_\_\_\_\_  
(подпись) (И.О. Фамилия)

**II. Рабочая программа пересмотрена на заседании департамента:**

Протокол от «\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_

Директор департамента \_\_\_\_\_  
(подпись) (И.О. Фамилия)

**III. Рабочая программа пересмотрена на заседании департамента:**

Протокол от «\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_

Директор департамента \_\_\_\_\_  
(подпись) (И.О. Фамилия)

**IV. Рабочая программа пересмотрена на заседании департамента:**

Протокол от «\_\_\_\_\_» \_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_

Директор департамента \_\_\_\_\_  
(подпись) (И.О. Фамилия)

## АННОТАЦИЯ

Рабочая программа учебной дисциплины **Технологии защиты информации** разработан для студентов, обучающихся по направлению подготовки— **09.03.03 Прикладная информатика**.

При изучении дисциплины охватывается следующий круг вопросов: классические математические проблемы и построение на их базе алгоритмов шифрования, эллиптические кривые, электронной цифровой подписью, хеширование файлов для сохранения целостности данных, алгоритмы с открытым и закрытым ключами.

Курс включает в себя следующие основные темы:

1. Классическая криптография.
2. Системы шифрования с открытым ключом
3. Алгоритмы факторизации
4. Криптографические алгоритмы, основанные на задаче дискретного логарифмирования в конечном поле
5. Эллиптические кривые и их приложения в криптографии
6. Отображения Вейля и Тейта

В рамках этого курса демонстрируется применение математических методов к формированию алгоритмов и протоколов, связанных с защитой информации. В курсе используются навыки и умения, полученные на предыдущих стадиях подготовки в рамках таких предметов, как дискретная математика, алгебра, теория вероятностей, языки программирования.

**Цель** изучения курса является освоение математических основ криптологии и принципов защиты информации при ее хранении, обработке и передаче, а также совершенствование навыков решения задач с использованием компьютера.

### **Задачи:**

4. Изучение математических основ криптологии.
5. Выработка умений для анализа и реализации в виде программного обеспечения алгоритмов и протоколов, используемых при защите информации.

6. Формирование представлений о роли информационных технологий в жизни общества.

Для успешного изучения дисциплины «Математические методы защиты информации» у обучающихся должны быть сформированы следующие предварительные компетенции:

способность приобретать и использовать организационно-управленческие навыки в профессиональной и социальной деятельности (ПК-8);

способность к самостоятельной научно-исследовательской работе (ОПК-3).

В результате изучения данной дисциплины у обучающихся формируются следующие общекультурные/ общепрофессиональные/ профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	Этапы формирования компетенции	
ПК-1 Способность создавать и сопровождать требования и технические задания на разработку, и модернизацию систем и подсистем малого и среднего масштаба и сложности	знает	современные информационно-коммуникационные технологии
	умеет	использовать современные информационно-коммуникационные технологии
	владеет	навыками использования современных информационно-коммуникационные технологий
ПК-4 Способность изготавливать компоненты информационных систем, включая программные комплексы, базы данных и интерфейсы "человек - электронно-вычислительная машина",	знает	основные принципы математического моделирования в современном естествознании, технике и социальных науках;
	умеет	формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций
	владеет	навыками использования современных программных средств визуализации результатов с учетом представлений о последствиях своей профессиональной деятельности
	умеет	использовать современные информационно-коммуникационные технологии

использовать современные инструментальные средства разработки, и программно-технологические платформы информационных систем	владеет	навыками использования современных программных средств решения математических задач
---	---------	---

Для формирования вышеуказанных компетенций в рамках дисциплины «Технологии защиты информации» применяются следующие методы активного/ интерактивного обучения:

- мини-лекции с актуализацией изучаемого содержания,
- презентации с использованием доски, книг, видео, слайдов, компьютеров и т.п., с последующим обсуждением материалов,
- обратная связь с формированием общего представления об уровне владения знаниями студентов, актуальными для занятия,
- разминка с вопросами, ориентированными на выстраивание логической цепочки из полученных знаний (конструирование нового знания),
- коллективные решения творческих задач, которые требуют от студентов не простого воспроизводства информации, а творчества, поскольку задания содержат большой или меньший элемент неизвестности и имеют, как правило, несколько подходов,
- работа в малых группах (дает всем студентам возможность участвовать в работе, практиковать навыки сотрудничества, межличностного общения).

## **1. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА**

Классическая криптография (18 часов)

1. Системы шифрования с открытым ключом (3 часов)
2. Алгоритмы факторизации (3 часов)
3. Криптографические алгоритмы, основанные на задаче дискретного логарифмирования в конечном поле (4 часов)
4. Эллиптические кривые и их приложения в криптографии (4 часов)

## 5. Отображения Вейля и Тейта (4 часов)

## 2. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Математические методы защиты информации» представлено в Приложении 1 и включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы.

## IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Раздел I. Классическая криптография	ПК-3, 4	Знает	Практическая работа	Коллоквиум
			Умеет	Практическая работа	Коллоквиум
			Владеет	Практическая работа	Коллоквиум
2	Раздел II. Системы шифрования с открытым ключом	ПК-3, 4	Знает	Практическая работа	Коллоквиум
			Умеет	Практическая работа	Коллоквиум
			Владеет	Практическая работа	Коллоквиум
3	Раздел III. Алгоритмы факторизации	ПК-3, 4	Знает	Практическая работа	Коллоквиум
			Умеет	Практическая работа	Коллоквиум
			Владеет	Практическая работа	Коллоквиум

4	Раздел IV. Криптографические алгоритмы, основанные на задаче дискретного логарифмирования в конечном поле	ПК-3, 4	Знает	Практическая работа	Коллоквиум
			Умеет	Практическая работа	Коллоквиум
			Владеет	Практическая работа	Коллоквиум
5	Раздел V. Эллиптические кривые и их приложения в криптографии	ПК-3, 4	Знает	Практическая работа	Коллоквиум
			Умеет	Практическая работа	Коллоквиум
			Владеет	Практическая работа	Коллоквиум
6	Раздел VI. Отображения Вейля и Тейта	ПК-3, 4	Знает	Практическая работа	Коллоквиум
			Умеет	Практическая работа	Коллоквиум
			Владеет	Лабораторная Практическая работа	Коллоквиум

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

## **V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **Основная литература**

*(печатные и электронные издания)*

- [1] Agrawal M. *PRIMES is in P* / M.Agrawal, N.Kayal, N.Saxena.– Annals of Mathematics.– 2004, v.160, p. 781–793.
- [2] Atkin A. *Prime sieves using binary quadratic forms*/ A. Atkin, D. Bernstein.– <http://cr.yp.to/papers/primessieves-19990826.pdf>
- [3] Berstein D. *ECM using Edwards curves*/ D. Berstein, P. Birkner, T.Lange, C. Peters.–2008, p.1–40 <http://eecm.cr.yp.to/eecm-20100616.pdf>
- [4] Berstein D. *Faster addition and doubling on elliptic curves.*/ D. Berstein, T.Lange. in AsiaCrypt'2007, p.29–50
- [5] Berstein D. *Explicit-formulas Database.*/ D. Berstein, T.Lange. 2007 <http://hyperelliptic.org/EFD>

- [6] Bernstein D. *Starfish on Strike*/ D. Bernstein, P. Birkner, T.Lange, C. Peters.– LATINCRYPT 2010, edited by Michel Abdalla and Paulo S. L. M. Barreto. Lecture Notes in Computer Science 6212. Springer, 2010, p.61–80
- [7] Boldyreva A. *Efficient Threshold Signature, Multisignature and Blind Signature Schemes based on Diffie–Hellman–Group Signature Scheme*. Crypto' 2003, Lect.Not.Comp.Sci., p.31–46
- [8] Boneh D.,Franklin M. *Identity based encryption from the Weil pairing*. In J.Killan, editor, Proceeding of Crypto'2001, volume 2139, Lect.Notes in Comp.Sci., 2001, p.213–229
- [9] Brent R.P. *Some integer factorization algorithms using elliptic curves*/ R.P. Brent.– Austral.Comput.Sci.Comm, 1986, v.8, p. 149–163.
- [10] Buhler J.P. *Factoring integers with the number field sieve* / J. P. Buhler, H. W. Lenstra, C. Pomerance.– in The Development of the Number Field Sieve, Springer–Verlag, Berlin, Germany, 1993, p. 50–94.
- [11] Chaum D. *Zero-knowledge undeniable signatures*. In I.Damgard, editor, Advances in Cryptology–Crypto'90, Lect.Not.Comp.Sci., v.740, 1992, p.89-105
- Список литературы* 133
- [12] Cocks C. *An identity based encryption scheme based on quadratic residues*. Cryptography and Coding, 2001.
- [13] Cohen H. *A course in computational algebraic number theory* / H. Cohen.– Springer–Verlag, Berlin, 1993, 545 p.
- [14] Crandall R. *The prime numbers: a computational perspective* / R. Crandall, C. Pomerance.– sec.ed. Springer–Verlag, Berlin, 2005, 604 p.
- [15] Dunham W. *Euler : The Master of Us All*. Mathematical Association of America, 1999, 185 p.
- [16] Edwards H.M. *A normal form for elliptic curves*./ H.M. Edwards.–Bull. Amer. Math. Soc. 44 (2007), p. 393-422
- [17] Elkenbracht-Huising M. *An implementation of the Number Field Sieve* / M. Elkenbracht-Huising.– Experimental Mathematics, 1996, v.5, p. 231—253.
- [18] Gardner M. *A new kind of cipher that would take millions years to break* / M. Gardner.– Sci. Amer. 1977, p. 120–124.
- [19] Granville A. *Smooth numbers: Computational number theory and beyond*/ A. Granville.– Proc. of MSRI workshop, 2004, 268–363
- [20] Hackmann P. *Elementary Number Theory* / P. Hackmann.– HHH Publ, 2007, 411 p.
- [21] Ishmukhametov S.T. *On a number of products of two primes*./ S.T. Ishmukhametov, R. Rubtsova.–Abstracts of International Conference dedicated to 100-anniversary of V. V. Morozov, Kazan, 2011
- [22] Joux A. *A one round protocol for tripartite Diffie-Hellman*. / A. Joux.– Algorithmic Number Theory: 4-th International Symposium, ANT–IV, Lecture Notes in Computer Science, v.1838(2000), Springer–Verlag, p. 385–393.



Список литературы 134

- [23] Joux A. *The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems*.  
Proceedings of the 5th International Symposium on Algorithmic Number Theory, Springer-Verlag London, 2002, p.20–32
- [24] Lenstra H.W. *Factoring integers with elliptic curves* / H.W. Lenstra.– Ann.Math. v.126 (1987), p. 649–674.
- [25] Lenstra A. *The Development of the Number Field Sieve* / A. Lenstra and H. Lenstra (eds.).– Lect.Not.in Math.1554, Springer–Verlag, Berlin, 1993, 139 p.
- [26] Longa P. *Fast Point Arithmetic for Elliptic Curve Cryptography*/ P. Longa.– Presentation at CliCC, University of Ottawa, Ottawa, Canada, 2006.
- [27] Longa P. *ECC Point Arithmetic Formulae (EPAF): Jacobian coordinates*/ P. Longa, C. Gebotus. In Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2010), 2010.
- [28] Menezes A. *Reducing Elliptic Curve Logarithms to a Finite Field* / A. Menezes, T. Okamoto, S. Vanstone.– IEEE Trans. Info. Theory, v.39, 1993, p. 1639–1646.
- [29] Menezes A. *Elliptic Curve Public Key Cryptosystems* / A. Menezes.– 1993, 144 p.
- [30] Montgomery P.L. *Speeding the Pollard and Elliptic Curve Methods of Factorization.*  
P.L. Montgomery.– Mathematics of Computation, v.48, iss.177, 1987, p.234–264.
- [31] Montgomery P.L. *An FFT-extension of the Elliptic Curve Method of Factirization*  
/ P.L. Montgomery.– Doctoral Dissertation, 1992, Univ.Calif. USA, 118 p.
- [32] Pollard J.M. *Theorems on factorization and primality testing* / J.M. Pollard. – Proc.Cambridge Phil.Society. 1974, v.76, p. 521-578.

Список литературы 135

- [33] Pomerance C. *Smooth Numbers and the Quadratic Sieve* / C. Pomerance. – MSRI publications, v.44 – 2008, p. 69–82.
- [34] Shoup V. *A Computational Introduction to Number Theory and Algebra*/ V. Shoup. – Cambridge University Press, Sec.Edition, 2005, 600 p.  
<http://shoup.net/ntb/>
- [35] Venturi D. *Lecture Notes on Algorithmic Number Theory.*/ D. Venturi. – Springer-Verlag, New-York, Berlin, 2009, 217 p.
- [36] Washington L. *Elliptic Curves Number Theory and Cryptography* /L. Washington.  
– Series Discrete Mathematics and Its Applications, Chapman & Hall/CRC,second ed. 2008, 524 p.
- [37] Аграновский А.В. *Практическая криптография: алгоритмы и их программирование* / А.В. Аграновский, Р.А. Хади.– М.: Солон-Пресс, 2009, 256 с.

- [38] Айерленд К. *Классическое введение в современную теорию чисел.* / К. Айерленд, М. Роузен. – М.: Мир, 1987, 428 с.
- [39] Акритас А. *Основы компьютерной алгебры и приложениями.* / А. Акритас. – М.: Мир, 1994, 544 с.
- [40] Богопольский О.В. *Алгоритмическая теория чисел и элементы криптографии.* / О.В. Богопольский.– Спецкурс для студентов НГУ, Новосибирск, 2005, 35 с. / <http://math.nsc.ru/bogopolski/Articles/SpezkNumber.pdf>
- [41] Болотов А.А. *Элементарное введение в эллиптическую криптографию: протоколы криптографии на эллиптических кривых.* / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. – М.:КомКнига, 2004, 280 с.
- [42] Болотов А.А. *Алгоритмические основы эллиптической криптографии.* / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, Часовских А.А.. – М.:РГСУ, 2004, 499 с.
- Список литературы 136*
- [43] Борович З.И. *Теория чисел.* / З.И. Борович, И.Р. Шафаревич. – 3-е издание, М.: Наука, 1985, 504 с.
- [44] Ван дер Варден Б.Л. *Алгебра.* / Б.Л.ван дер Варден. – изд.2, М.: Наука, 1979, 623 с.
- [45] Василенко О.Н. *Теоретико-числовые алгоритмы в криптографии/* О.Н. Василенко. – МЦНМО, 2003, 326 с.
- [46] Вельценбах М. *Криптография на C и C++ в действии: учебное пособие* / М. Вельценбах. – М.: Триумф, 2008, 464 с.
- [47] Захаров В.М. *Вычисления в конечных полях: уч.-метод. пособие* / В.М. Захаров, Б.Ф. Эминов. – Казань: КГТУ им. А.Н.Туполева, 2010, 132 с.
- [48] Ишмухаметов Ш.Т. *Методы факторизации натуральных чисел/* Ш.Т.Ишмухаметов. – Казань, 2012, 189 с.
- [49] Коблиц Н. *Курс теории чисел и криптографии* / Н. Коблиц. – М.: ТВП, 2001, 260 с.
- [50] Корешков Н.А. *Теория чисел./*Н.А. Корешков. – Уч.-мет. пособие, Казань, КФУ, 2010, 35 с.
- [51] Кормен Т. *Алгоритмы: построение и анализ* /Т. Кормен, Ч. Лейзерсон, Р. Ривест. – М.: МЦНМО, 1999.
- [52] Лазарева С.В. *Математические основы криптологии: тесты простоты и факторизация* / С.В. Лазарева, А.А. Овчинников. Учебное пособие, Санкт-Петербург, СПбГУАП, 2006, 65 с.
- [53] Лидл Р. *Конечные поля/*Р. Лидл,Г. Нидеррайтер.– Т. 1, 2. М.: Мир, 1988, 428 с.
- [54] Молдовян Н.А. *Криптография. От примитивов к синтезу алгоритмов* / Н.А.Молдовян, А.А. Молдовян,М.А. Еремеев. – БХВ-Петербург, 2004, 446 с.
- 137
- [55] Нестеренко Ю.В. *Теория чисел/* Ю.В. Нестеренко. – Москва, Изд.Центр Академия, 2008, 273 с.

- [56] А.Г. Ростовцев, Е.Б. Маховенко. Теоретическая криптография, Профессионал, Санкт-Петербург, 2005, 479 с.
- [57] Сизый С.В. *Лекции по теории чисел: учебное пособие для математических специальностей* / С.В. Сизый.– Екатеринбург, УрГУ, 1999, 136 с.
- [58] Чандрасекхаран К. *Введение в аналитическую теорию чисел* / К. Чандрасекхаран.–М.– Мир, 1974, 187 с.
- [59] Черемушкин А.В. *Лекции по арифметическим функциям в криптографии* / А.В. Черемушкин.– М.: МЦНМО, 2002, 103 с.
- [60] ) Шаньгин Ф.Ф. *Защита компьютерной информации: эффективные методы и средства* /Ф.Ф. Шаньгин.– М.:ДМК, 2008, 542 с.

### **Дополнительная литература**

*(печатные и электронные издания)*

1. Осипян В. О., Осипян К. В. Криптография в упражнениях и задачах  
Издательство: Гелиос АРВ, 2004.
2. Скембрей Дж, Мак-Клар С., Курц Дж. Секреты хакеров. Безопасность сетей - готовые решения. М.: Изд. дом Вильямс, 2001.
3. Ноден П., Китте К. Алгебраическая алгоритмика (с упражнениями и решениями). - М.: Мир, 1994
4. Введение в криптографию /Под общ. ред. В. В. Яценко. - М.: МЦНМО: "ЧеРо", 1999.
5. Фергюсон Н., Шнайдер Б. Практическая криптография. -- М.: Вильямс, 2005.
6. Материалы, посвященные книге Столлинс В. "Криптография и защита сетей: принципы и практика".

## **VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ**

**Рекомендации по планированию и организации времени, необходимого для изучения дисциплины.** Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

Выполнить домашнее задание по теме практического занятия – 1-2 часа в неделю.

Оформить отчет о выполнении заданий лабораторной работы – 1-2 часа.

Тогда общие затраты времени на освоение курса «Технологии защиты информации» студентами составят 2-4 часа в неделю.

**Описание последовательности действий студента («сценарий изучения дисциплины»).** При выполнении самостоятельной работы рекомендуется изучить теоретический материал лекционного занятия, методы решения задач на практическом занятии, теоретические основы методов, изученных в ходе лабораторной работы:

В течение недели выбрать время для оформления результатов лабораторной работы.

После практического занятия рекомендуется выполнить домашние задания для закрепления навыков и подготовки к выполнению контрольных заданий.

**Рекомендации по использованию материалов учебно-методического комплекса.** Рекомендуется использовать методические указания по выполнению лабораторных работ и материалы по курсу «Криптографические методы защиты информации».

**Указания по организации работы с контрольно-измерительными материалами.** Рекомендуется представлять отчеты по лабораторным работам в соответствии с методическими рекомендациями по их выполнению.

## **VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Учебные аудитории для проведения лабораторных занятий с настольными компьютерами и установленном на них программном обеспечением QGIS и/или GRASS GIS.

## План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1 неделя	Практическая работа № 1	2 часа	Письменный отчет
2	1 неделя	Практическая работа №2	2 часа	Письменный отчет
3	2 неделя	Практическая работа №3	2 часа	Письменный отчет
4	3 неделя	Практическая работа №4	2 часа	Письменный отчет
5	3 неделя	Практическая работа №5	2 часа	Письменный отчет
6	4 неделя	Практическая работа №6	2 часа	Письменный отчет
7	5 неделя	Практическая работа №7	2 часа	Письменный отчет
8	5 неделя	Практическая работа №8	2 часа	Письменный отчет
9	6 неделя	Практическая работа №9	2 часа	Письменный отчет
10	7 неделя	Практическая работа №10	2 часа	Письменный отчет
11	7 неделя	Практическая работа №11	2 часа	Письменный отчет
12	8 неделя	Практическая работа №12	2 часа	Письменный отчет
13	9 неделя	Практическая работа №13	2 часа	Письменный отчет
14	9 неделя	Практическая работа №14	2 часа	Письменный отчет
15	10 неделя	Практическая работа №15	2 часа	Письменный отчет
16	11 неделя	Практическая работа №16	2 часа	Письменный отчет
17	11 неделя	Практическая работа №17	2 часа	Письменный отчет
18	12 неделя	Практическая работа №18	2 часа	Письменный отчет

19	13 неделя	Практическая работа №19	2 часа	Письменный отчет
20	13 неделя	Практическая работа №20	2 часа	Письменный отчет
21	14 неделя	Практическая работа №21	2 часа	Письменный отчет
22	15 неделя	Практическая работа №22	2 часа	Письменный отчет
23	15 неделя	Практическая работа №23	2 часа	Письменный отчет
24	16 неделя	Практическая работа №24	2 часа	Письменный отчет
25	17 неделя	Практическая работа №25	2 часа	Письменный отчет
26	17 неделя	Практическая работа №26	2 часа	Письменный отчет
27	18 неделя	Практическая работа №27	2 часа	Письменный отчет

## **Рекомендации по самостоятельной работе студентов**

Самостоятельная работа студентов состоит из решения задач и подготовки реферата по согласованной теме.

### **Основные требования к содержанию реферата**

Студент должен использовать только те материалы (научные статьи, монографии, пособия), которые имеют прямое отношение к избранной им теме.

По своей *структуре* реферат состоит из:

1. Введения, где студент формулирует проблему, подлежащую анализу и исследованию;
2. Основного текста, в котором последовательно раскрывается избранная тема. Возможно описание фрагментов кода, который разрабатывается в процессе подготовки реферата.
3. Заключение, где студент формулирует выводы, сделанные на основе основного текста.

4. Списка использованной литературы. В данной список включаются все источники, на которые имеются ссылки в тексте. Использование материалов Википедии является нежелательным.

### **Порядок сдачи реферата и его оценка**

Реферат готовится студентами в течение семестра по тематике, согласуемой по почте. Защита рефератов проводится в рамках лабораторных работ. При защите реферата студент должен дать разъяснения и ответить на вопросы по тексту.

### **Тематика рефератов**

1. Парадокс дней рождений
2. Китайская теорема об остатках
3. Гипотеза Римана

## Рефераты

Реферат объемом 2 стр. без обложки должен быть представлен и защищен до экзамена/зачета по согласованной теме (темы, предварительный список литературы и содержание для согласования нужно присылать по почте). Основное направление -- криптоанализ и отдельные составляющие изученных систем, а также современные криптографические протоколы, криптографические системы и т. п., которые не были затронуты на лекциях. Требуется подобрать и изучить современные источники и попытаться на двух стр. самостоятельно изложить материал со ссылками на библиографические описания использованных источников. Любое заимствование должно быть явно обозначено. Примеры рефератов, подготовленных в предыдущие годы, доступны на сайте (Алгоритм шифрования IDEA, Коллизии хэш-функций, Схема разделения секрета Шамира, протоколы для обеспечения секретности и идентификации и т. д.).

## Паспорт ФОС

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Раздел I. Классическая криптография	ПК-3, 4	Знает	Лабораторная работа	Коллоквиум
			Умеет	Лабораторная работа	Коллоквиум
			Владеет	Лабораторная работа	Коллоквиум
2	Раздел II. Системы шифрования с открытым ключом	ПК-3, 4	Знает	Лабораторная работа	Коллоквиум
			Умеет	Лабораторная работа	Коллоквиум
			Владеет	Лабораторная работа	Коллоквиум
3	Раздел III. Алгоритмы факторизации	ПК-3, 4	Знает	Лабораторная работа	Коллоквиум
			Умеет	Лабораторная работа	Коллоквиум
			Владеет	Лабораторная работа	Коллоквиум



				работа	
4	Раздел IV. Криптографические алгоритмы, основанные на задаче дискретного логарифмирования в конечном поле	ПК-3, 4	Знает	Лабораторная работа	Коллоквиум
			Умеет	Лабораторная работа	Коллоквиум
			Владеет	Лабораторная работа	Коллоквиум
5	Раздел V. Эллиптические кривые и их приложения в криптографии	ПК-3, 4	Знает	Лабораторная работа	Коллоквиум
			Умеет	Лабораторная работа	Коллоквиум
			Владеет	Лабораторная работа	Коллоквиум
6	Раздел VI. Отображения Вейля и Тейта	ПК-3, 4	Знает	Лабораторная работа	Коллоквиум
			Умеет	Лабораторная работа	Коллоквиум
			Владеет	Лабораторная работа	Коллоквиум

### Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	Этапы формирования компетенции		критерии	показатели	баллы
ПК-3 Способность создавать и сопровождать требования и технические задания на разработку, и модернизацию систем и подсистем малого и среднего масштаба и сложности	знает	современные информационно-коммуникационные технологии	представление о современных информационно-коммуникационных технологиях	знание основных требований информационной безопасности	45-64
	умеет	использовать современные информационно-коммуникационные технологии	умение использовать современные информационно-коммуникационные технологии	умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационно	65-79

	владеет	навыками использования современных информационно-коммуникационные технологии	владение навыками использования современных информационно-коммуникационные технологии	й безопасности применение навыков решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	80-100
ПК-4 Способность изготавливать компоненты информационных систем, включая программные комплексы, базы данных и интерфейсы "человек - электронно-вычислительная машина", использовать современные инструментальные средства разработки, и программно-технологические платформы информационных систем	знает	основные принципы математического моделирования в современном естествознании, технике и социальных науках; базовые методы и математические модели в выбранной предметной области;	представление об основных принципах математического моделирования в современном естествознании, технике и социальных науках;	знание базовых методов и математических моделей современного естествознания	45-64
	умеет	формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций	умение формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций	умение создавать алгоритмы решения задач, представлять итоги проделанной работы в виде отчетов с учетом социальных, профессиональных и этических позиций	65-79
	владеет	навыками использования современных программных средств решения математических задач и	применение навыков использования программных средств для решения математических	систематическое применение навыков работы с учетом представлений о последствиях своей	80-100

		визуализации результатов с учетом представлений о последствиях своей профессиональной деятельности	задач с учетом представлений о последствиях своей профессиональной деятельности	профессиональной деятельности	
--	--	--	---	-------------------------------	--

### Оценочные средства для текущей аттестации

Приводятся типовые оценочные средства для текущей аттестации и критерии оценки к ним (по каждому виду оценочных средств) в соответствии с Положением о фондах оценочных средств образовательных программ высшего образования – программ бакалавриата, специалитета, магистратуры ДВФУ, утвержденным приказом ректора от 12.05.2015 №12-13-850.

- 100-86 баллов выставляется, если студент/группа точно определили содержание и составляющие части задания, умеют аргументированно отвечать на вопросы, связанные с заданием. Продемонстрировано знание и владение навыками самостоятельной исследовательской работы по теме. Фактических ошибок, связанных с пониманием проблемы, нет.

- 85-76 – баллов работа студента/группы характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет.

- 75-61 балл – проведен достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимание базовых основ и теоретического обоснования выбранной темы. Привлечены основные источники по рассматриваемой теме. Допущено не более 2 ошибок в смысле или содержании проблемы

- 60-50 баллов – если работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Допущено три или более трех ошибок смыслового содержания раскрываемой проблемы

### Шкала оценивания

Менее 60 баллов	незачтено	неудовлетворительно
От 61 до 75 баллов	зачтено	удовлетворительно

От 76 до 85 баллов	зачтено	хорошо
От 86 до 100 баллов	зачтено	отлично

### Вопросы к экзамену

1. Основные понятия информационной безопасности. Методы информационной безопасности. Сервисы информационной безопасности. Угрозы информационной безопасности. Классификация криптографических методов защиты информации
2. Модулярная арифметика. Функция Эйлера $\varphi(n)$
3. Особенности систем с открытым ключом. Алгоритм RSA
4. Расширенный алгоритм Евклида
5. Алгоритм быстрого возведения в степень по модулю
6. Генерация простых чисел. Решето Эратосфена
7. Метод пробных делений
8. Решето Аткина
9. Тест Поклингтона
10. Символ Лежандра
11. Тест простоты Миллера–Рабина
12. Вероятностный тест простоты Соловея–Штрассена
13. Китайская теорема об остатках
14. Протокол Диффи-Хеллмана
15. Электронная цифровая подпись и ее свойства
16. Односторонние функции. Хеш-функции
17. Алгоритм создания электронной цифровой подписи
18. Алгоритм построения ЭЦП Эль-Гамала
19. Эллиптические кривые и их приложения в криптографии. Определение эллиптической кривой