**Программа учебной дисциплины «НИС «Методы и алгоритмы защиты информации»**

Утверждена

Академическим советом ООП

Протокол № от «\_\_»\_\_\_\_\_20\_\_ г.

|  |  |
| --- | --- |
| Автор  | Набебин А.А., к.ф.-м.н., доцент, anabebin@hse.ru |
| Число кредитов  | 3 |
| Контактная работа (час.)  | 56 |
| Самостоятельная работа (час.)  | 58 |
| Курс  | 1 |
| Формат изучения дисциплины | без использования онлайн курса |

1. **ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ**

Цели освоения дисциплины «Методы и алгоритмы защиты информации»:

* формирование у студентов профессиональных компетенций, связанных с общей методологией научного исследования;
* формирование у студентов профессиональных компетенций, связанных с частными аспектами анализа, исследования и разработки криптографических ресурсно-эффективных комбинированных протоколов (алгоритмов);
* приобретение практических навыков самостоятельного научного исследования в области создания эффективных криптосистем для решения задач защиты информации;
* развитие умений, основанных на полученных теоретических знаниях, позволяющих на творческом и репродуктивном уровне применять и создавать эффективные криптографические алгоритмы для решения задач защиты информации;
* получение студентам навыков самостоятельной исследовательской работы, предполагающей изучение специфических методов анализа криптоалгоритмов, инструментов и средств, необходимых для решения актуальной, в аспекте программной инженерии, задачи выбора рациональных алгоритмов, в зависимости от особенностей применения разрабатываемых защищающих средств.

В результате освоения дисциплины студент должен:

 Знать:

— необходимые сведения из модулярной арифметики (теории сравнений) целых чисел;

— основные понятия абстрактной алгебры, теоремы и алгоритмы в конечных группах, (полиномиальных) кольцах и полях;

— основные алгоритмы модулярной арифметики целых чисел и полиномов (НОД, НОК, модулярная степень, тесты на простоту натуральных чисел, неприводимость и примитивность полиномов в конечных полиномиальных полях);

— основные шифровальные систем и электронные цифровые подписи (ЭЦП) с открытым ключом (RSA, Эль-Гамаля, DSA), основанные на фактах модулярной алгебры целых чисел и конечных полиномиальных полей;

— подходы к разработке шифросистем и ЭЦП с открытым ключом основанных на группах точек эллиптических кривых, на группах кос, в мнимых квадратичных полях, в частично упорядоченных множествах;

 Уметь:

— оценивать компьютерные криптографические протоколы (алгоритмы) с

 использованием комплексных крите­риев качества, в том числе оценивать

 ресурсную эффективность алгоритмов;

— пользоваться базовыми умениями и навыками ведения самостоятельных

 исследований на примере анализа криптографических протоколов (алгоритмов);

— пользоваться теорией защиты информации для решения прикладных задач

 информатики;

— выступать с научными докладами, оформлять содержательные презентации и

 корректно вести научные дискуссии.

 Иметь навыки (приобрести опыт):

— оценки трудоемкости криптографических протоколов;

— экспериментального исследования программных реа­лизаций

 криптографических алгоритмов;

— в поиске подходов к разработке эффективных комбинированных

 криптографических алгорит­мов на основе их сравнительного анализа и

 умение применять их при разработке алгоритмов решения практических

 задач защиты информации.

Изучение данной дисциплины базируется на знаниях, полученных студентами при освоении учебных дисциплин «Дискретная математика», «Программирование».

Дисциплина является основой для последующего изучения дисциплин: «Спецификация программных систем», научно-исследовательского семинара «Верификация программных систем».

1. **СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**Тема 1.** Модулярная арифметика (теория сравнений) целых чисел. Теоремы и алгоритмы в конечных группах, (полиномиальных) кольцах и полях.

**Тема 2.** Основные алгоритмы модулярной арифметики целых чисел и полиномов (НОД, НОК, модулярная степень, тесты на простоту натуральных чисел, неприводимость и примитивность полиномов в конечных полиномиальных полях).

**Тема 3.** Квадратичные вычеты. Символы Лежандра и Якоби. Примитивные корни и индексы. Дискретный логарифм.

**Тема 4.** Криптосистемы RSA, ЭльГамаля, DSA..

**Тема 5.** Группы точек эллиптических кривых, теории кос, решеток частично упорядоченных множеств

**Тема 6.** Блоковые и потоковые шифры.

1. **ОЦЕНИВАНИЕ**

# Формы контроля знаний студентов

|  |  |  |  |
| --- | --- | --- | --- |
| Тип контроля | Форма контроля | модули | Параметры  |
| 1 | 2 | 3 | 4 |
| Текущий(неделя) | Домашнее задание  |  | \* | \* | \* | Абстрактная алгебра, криптопротоколы |
| Итоговый | Экзамен |  |  |  | \* | 60 мин. |

# Порядок формирования оценок по дисциплине

Оценки по всем формам контроля выставляются по 10-ти балльной шкале.

Оценки текущего и итогового контроля складываются из следующих элементов.

*Текущий контроль*

Оценка *Тк* в 10-бальной системе ставится за качество подготовки и работы на семинарских занятиях (доклады, презентации, оппонирование, критические выступления, выполнение домашних заданий); при непосещении занятий ставится оценка «0».

*Индивидуальное домашнее задание*

Задание сдается в виде еженедельных отчетов в письменной и в электронной форме. Каждая задача индивидуального задания оценивается в 10-ти бальной системе. Позже сданное домашнее задание оценивается ниже, чем задание во время сданное. Все задачи домашнего задания должны быть сданы полностью. Оценка *Д* выполненного домашнего задания есть среднее арифметическое всех оценок за каждую задачу.

*Итоговый контроль*

Экзамен в конце четвертого модуля проходит в форме собеседования, при пропуске экзамена ставится оценка «0».

*накопленная оценка Н за дисциплину* по 10-балльной шкале формируется как взвешенная сумма: *Н* = 0.2*Тк* + 0.8 *Дз*,

*результирующая оценка за дисциплину* *К* по 10-балльной шкале формируется как взвешенная сумма:

*K* = 0.8 *Н* + 0.2 *З*, где *Тк,* *Дз, З* есть 10-балльные оценки за текущий контроль, домашнее задание и за экзамен. Перевод в пятибалльную оценку осуществляется в соответствии со следующей таблицей.

**Таблица соответствия оценок по десятибалльной и пятибалльной системам**

|  |  |
| --- | --- |
| **По десятибалльной шкале** | **По пятибалльной шкале** |
| 1 – неудовлетворительно2 – очень плохо3 – плохо | неудовлетворительно – 2  |
| 4 – удовлетворительно5 – весьма удовлетворительно | удовлетворительно – 3  |
| 6 – хорошо7 – очень хорошо | хорошо – 4  |
| 8 – почти отлично9 – отлично10 – блестяще | отлично – 5  |

1. **ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ**

# Оценочные средства для текущего контроля студента

***Домашнее задание***

1. Даны целые числа *a* = 100+*N* ( *N* есть номер фамилии студента в аудиторном журнале) и *b*=11. Найти целые, *q*1, *q*2, *r*1, *r*2,  *r*1, *r*2 < *b*, для которых  *a* = *bq1* + *r*1, –*a* = *bq*2 + *r*2.
2. Записать данные числа в восьмеричной, шестеричной, десятичной системах счисления.
3. Записать десятичные числа *n=*100*+N*, *m=*200*+N* в семеричной и двоичной системах счисления*. N* есть номер фамилии студента в аудиторном журнале.
4. Перемножить числа из задачи 3 в системе счисления по основанию семь.
5. В двоичной системе счисления разделить число из задачи 2 на число 1011012.
6. Найти число цифр в десятичном числе *n* по основаниям 2, 3, 5, 7, 8, 12, 16. В качестве числа написать свою фамилию и взять из записи начальный отрезок длины 5. Если длина записи меньше пяти, то дописать букву «ю» необходимое число раз. Пусть получили слово *s* (длины 5). Все 32 буквы русского алфавита пронумеруем по порядку от 1 до 32. Пробел есть 0. Тогда слово *s* можно рассматривать как число в системе счисления по основанию 33. Число *n* получается переводом *s*32 в десятичное число.
7. Разложить данное число *n* на простые множители и найти число делителей *f*(*n*) числа *n*.
8. Найти наибольший общий делитель *d* и наименьшее общее кратное чисел *a* и *b*. Число *a* взять из задачи 6, число *b*=780. Найти те *u* и *v*, для которых *d* = *ua* + *vb*.
9. Найти непрерывные и подходящие дроби для числа *a*/*b*, *a*  *b*.
10. Написать полную, наименьшую по модулю, приведенную системы вычетов по данному модулю *n*. Для полной и приведенной системы вычетов написать таблицы сложения, умножения. Написать каноническое разложение числа *n* вычислить для него функцию Эйлера **(*n*). Для полной системы вычетов написать по умножению таблицу обратных элементов, таблицу степеней до показателя **(*n*) и указать порядок каждого элемента. Для *n* указать генератор (по умножению), если он существует.
11. Найти степень 5613+*N* (mod 1135), где *N* есть номер, под которым стоит фамилия студента в аудиторном журнале.
12. Решить (подбором) сравнения.
13. Решить (подбором) систему из двух сравнений с одним неизвестным.
14. Решить (подбором) систему из двух сравнений с двумя неизвестными.
15. Решить (методом Гаусса) систему из трех сравнений.
16. Решить систему из трех сравнений типа *x* ≡ *b* (mod *m*).
17. Решить систему из трех сравнений типа *ax* ≡ *b* (mod *m*).
18. Определить с помощью символа Лежандра, имеет ли решение данное сравнение.
19. Определить с помощью символа Якоби, имеет ли решение данное сравнение.
20. Полиномы  *f*(*x*), *g*(*x*)  5[*x*].
21. Найти их наибольший делитель *d*(*x*) = нод(*f*(*x*), *g*(*x*)) и те полиномы *u*(*x*),*v*(*x*)  5[*x*], для которых *d*(*x*) = *f*(*x*)*u*(*x*) + *g*(*x*)*v*(*x*). Полином *f*(*x*)  *p*[x] степени *m* над простым полем*p*, *p=5,*  *m* =2, задан как определяемое вариантом натуральное число *a*. Например, для *a* = 10810 = 4135 полином  *f*(*x*) = 4·*x*2 + 1·*x* + 3 = 4*x*2 + *x* + 3.

 a) по заданному числу *a* найти полином *f*(*x*)  *p*[x].

 b)построить таблицу значений для *f*(*x*) и проверить, будет ли полином *f*(*x*) над полем *p* неприводим.

 c) написать все элементы поля *GF*(*pm*) =*p*[*x*]/(*f*(*x*)) из *q* = *pm* из *pm* остатков от деления полиномов из*p*[*x*] на модуль *f*(*x*).

 d) для поля *GF*(*pm*) =*p*[*x*]/(*f*(*x*)) из *q* = *pm* остатков от деления полиномов из*p*[*x*] на *f*(*x*) построить таблицы для сложения и умножения элементов *a*1*x* + *a*0, *a*1 = 3, *a*0  5, на все элементы поля *GF*(*pm*).

 e) для каждого элемента *a*1*x* + *a*0, *a*1 = 3, *a*0  5, указать обратный (по умножению) элемент.

 22. Найти степень (по умножению) элемента поля *GF*(*pm*) и указать, является ли заданный

 элемент генератором для *GF*(*pm*). Элемент поля *a*1*x* + *a*0 задан как вектор *a*1*a*0.

23. Зашифровать и расшифровать сообщение с помощью криптосистемы RSA.

24. Подписать сообщение с помощью ЭЦП RSA.

25. Зашифровать и расшифровать сообщение с помощью числовой криптосистемы Эль-Гамаля.

26. Подписать сообщение с помощью числовой ЭЦП Эль-Гамаля.

27. Зашифровать и расшифровать сообщение с помощью полиномиальной криптосистемы Эль-Гамаля.

28. Подписать сообщение с помощью полиномиальной ЭЦП Эль-Гамаля.

29. Подписать сообщение с помощью ЭЦП DSA.

Оценочные средства для промежуточной аттестации

1. Делимость и ее свойства. Представление числа по делителю, частному, остатку. Представление числа в системе счисления по основанию *h*.
2. Простые числа. Бесконечность множества простых чисел. Решето Эратосфена для простых чисел.
3. Теорема о факторизации и ее свойства.
4. Наибольший общий делитель (НОД) и его свойства. Вычисление НОД с помощью теоремы о факторизации. Алгоритм Евклида вычисления НОД. Расширенный алгоритм Евклида.
5. Наименьшее общее кратное (НОК) и его свойства. Вычисление НОК с помощью теоремы о факторизации. Связь между НОД и НОК.
6. Непрерывные и подходящие дроби и их вычисление.
7. Целая и дробная часть вещественного числа. Мультипликативная функция. Сумма мультипликативной функции от числа по всем делителям этого числа.
8. Функция Мебиуса. Преобразование Мебиуса.
9. Функция Эйлера и ее вычисление.
10. Сравнение целых чисел. Три определения сравнений и их эквивалентность. Свойства сравнений.
11. Полная система вычетов. Наименьшая неотрицательная, абсолютно наименьшая, приведенная система вычетов. Классы вычетов. Операции над классами.
12. Теоремы Эйлера и Ферма.
13. Сравнения с одним неизвестным произвольной степени. Решение сравнения. Система сравнений произвольных степеней и ее решение.
14. Сравнения и их системы с несколькими переменными и их решение.
15. Сравнения первой степени и их решение.
16. Система сравнений первой степени. Теорема Гаусса о ее решении.
17. Сравнения любой степени по простому модулю и их решение. Теорема Вильсона.
18. Сравнения любой степени по составному модулю и их решение.
19. Вычеты (корни) степени *n*. Квадратичные вычеты (квадратные корни) и их свойства. Квадратичные вычеты по простому модулю.
20. Символ Лежандра и его свойства.
21. Символ Якоби и его свойства.
22. Квадратичные вычеты (квадратные корни) по составному модулю.
23. Числа и их экспоненты (показатели) по данному модулю. Связь между сравнением степеней и их экспонент.
24. Примитивные (первообразные) корни и их свойства. Теорема о существовании примитивных корней.
25. Универсальные алгебры. Гомоморфизм и изоморфизм алгебр. Теорема о гомоморфизме.
26. Полугруппы, подполугруппы, циклические полугруппы.
27. Кольца и поля. Характеристика поля. Конечные поля.
28. **РЕСУРСЫ**
	1. **Основная литература**

• **Набебин А.А.** Дискретная математика. М.: Научный мир, 2010. 512с. (Доступна в

 библиотеке НИУ ВШЭ).

• **Набебин А.А**. Сборник заданий по дискретной математике. М.: Научный мир, 2009. 280с.

 (Доступна в библиотеке НИУ ВШЭ).

* 1. **Дополнительная литература**

• **Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В**. Основы криптографии.

 М.: Гелиос АРВ, 2002.

• **Бабаш А.В**. Криптографические и теоретико-автоматные аспекты современной защиты

 информации. М.: Издат. центр ЕАОИ, том 1, 2008; том 2, 2008; том 3, 2010.

• **Болотов А.А., Гашков С.Б., Фролов А.Б. Часовских А.А**. Элементарное введение в

 эллиптическую криптографию. Алгебраические и алгоритмические основы. М.: КомКнига,

 2006.

• **Болотов А.А., Гашков С.Б., Фролов А.Б.** Элементарное введение в эллиптическую

 криптографию. Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006.

• **Виноградов И.М**. Основы теории чисел. СПБ.: Лань, 2004.

• **Лидл Р., Нидеррайтер Г**. Конечные поля. М.: Мир, 1988.

• **Новиков Ф.А**. Дискретная математика для программистов – СПб.: Питер 2008. – 304 с.

• **Разборов А.А.** О сложности вычислений — Математическое просвещение — сер. 3, вып.

 3, 1991 г. <http://www.mccme.ru/free-books/matpros/i4127141.pdf.zip>.

• **Смарт Н**. Криптография. М.: Техносфера, 2005.

• **Шнейер Б**. Прикладная криптография. М.: Триумф, 2002.

* 1. **Материально-техническое обеспечение дисциплины**

ПЭВМ с доступом в Интернет (операционная система, офисные программы, антивирусные программы);

мультимедийный проектор с дистанционным управлением.