МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
Государственное образовательное учреждение высшего образования Московской области
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ОБЛАСТНОЙ УНИВЕРСИТЕТ
(МГОУ)

Факультет физико-математический

Кафедра вычислительной математики и методики преподавания информатики

УТВЕРЖДЕН на заседании кафедры
Протокол «20» мая 2020 г. № 10

Зав. кафедрой _____ /Шевчук М.В./

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине
**Математические основы защиты информации и информационной безопасности**

Направление подготовки
**44.04.01 Педагогическое образование**

Программа подготовки
**Информатика в образовании**

Мытищи
2020

Авторы-составители:

Шевчук Михаил Валерьевич,
кандидат физико-математических наук,
доцент кафедры вычислительной математики и методики преподавания информатики

Шевченко Виктория Геннадьевна,
кандидат педагогических наук,
доцент кафедры вычислительной математики и методики преподавания информатики

Фонд оценочных средств по дисциплине «Математические основы защиты информации и информационной безопасности» составлен в соответствии с требованиями Федерального Государственного образовательного стандарта высшего образования (№ 126 от 22.02.2018) по направлению подготовки 44.04.01 Педагогическое образование, программа подготовки «Информатика в образовании».

Дисциплина входит в блок факультативных дисциплин и является дисциплиной по выбору.

**Год начала подготовки 2020**

**1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы**

| Код и наименование компетенции | Этапы формирования |
|---|---|
| СПК-6 «Способен самостоятельно осуществлять научное исследование и применять его результаты при решении конкретных научно-исследовательских задач» | 1. Работа на учебных занятиях.<br>2. Самостоятельная работа. |

**2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания**

| Оцениваемые компетенции | Уровень сформированности | Этап формирования | Описание показателей | Критерии оценивания | Шкала оценивания |
|---|---|---|---|---|---|
| СПК-6 | Пороговый | 1. Работа на учебных занятиях (лекции, лабораторные занятия) Тема 1-8<br>2. Самостоятельная работа (выполнение домашних заданий) | Знать:<br>-<br>Уметь:<br>- | Тестирование<br>Лабораторная работа | Шкала оценивания тестирования<br>Шкала оценивания лабораторной работы |
| | Продвинутый | 1. Работа на учебных занятиях (лекции, лабораторные занятия) Тема 1-8<br>2. Самостоятельная работа (выполнение лабораторных работ, выполнение домашних заданий) | Знать:<br>-<br>Уметь:<br>-<br>Владеть:<br>- | Тестирование<br>Лабораторная работа | Шкала оценивания тестирования<br>Шкала оценивания лабораторной работы |

**3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы**

**Примерные вопросы для тестовых заданий**

*Выберите один правильный ответ.*

1. Документ, в котором информация представлена в электронно-цифровой форме:
   a) электронная цифровая подпись
   b) быстрая цифровая подпись
   c) электронный документ

*Выберите один правильный ответ.*

2. Что входит в схему электронной подписи:
   a) алгоритм генерации ключевых пар пользователя
   b) функции обработки подписи
   c) функцию вычисления подписи
   d) функцию удаления подписи
   e) функцию проверки подписи

*Выберите один правильный ответ.*

3. Для чего в асимметричном методе шифрования используется несекретный
   a) расшифрования
   b) шифрования
   c) аутентификации
   d) конфиденциальности

4. *Соотнесите* понятия и определения:

| | |
|---|---|
| 1) Код | a) Операция, обратная кодированию, восстановление информации в первичном алфавите по полученной последовательности кодов. |
| 2) Кодирование | b) Знаки вторичного алфавита, используемы для представления знаков или их сочетаний первичного алфавита |
| 3) Декодирование | c) Перевод информации, представленной посредством первичного алфавита, в последовательность кодов. |

*Выберите один правильный ответ.*

5. Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации _ это…
   a) электронный документ
   b) электронная цифровая подпись
   c) ключ электронной цифровой подписи

*Выберите один правильный ответ.*

6. Какие ключи используются в асимметричном методе шифрования:
   a) секретный
   b) несекретный
   c) секретный и несекретный

*Выберите один правильный ответ.*

7. Для чего в асимметричном методе шифрования используется секретный ключ:
   a) расшифрования
   b) шифрования
   c) аутентификации
   d) конфиденциальности

*Выберите один правильный ответ.*

8. 1 байт = ... бит.
   a) 8
   b) 16
   c) 4
   d) 32

*Вставьте пропущенное слов.*

9. _____ - раздел математики, в котором изучаются и разрабатываются системы изменения письма с целью сделать его непонятным для непосвященных лиц.

**Примерный вариант практической работы**

1. Создать контрольные суммы для любых пяти файлов, используя методы

хеширования с помощью HashTab согласно варианту из таблицы заданий (стр. 87) и заполнить таблицу результатов:

| | Алгоритм | Расшифровка | Значение хеш-сумм |
|---|---|---|---|
| Название_файла1.расширение | | | |
| | | | |
| | | | |
| | | | |
| Название_файла2.расширение | | | |
| | | | |
| | | | |
| | | | |
| Название_файла3.расширение | | | |
| | | | |
| | | | |
| | | | |
| Название_файла4.расширение | | | |
| | | | |
| | | | |
| | | | |
| Название_файла5.расширение | | | |
| | | | |
| | | | |
| | | | |

2. Сравнить контрольные суммы MD5 пяти любых файлов, созданные с помощью HashTab и FreeCommander, результаты представить в таблице:

3.

| № | Название файла с расширением | FreeCommander | HashTab |
|---|---|---|---|
| | | | |

**Примерные вопросы к зачету (проводится в устной форме)**

1. Основные понятия криптографии.
2. Подстановочные шифры.
3. Перестановочные шифры.
4. Компьютерные алгоритмы.
5. Основные криптографические протоколы.
6. Передача информации с использованием симметричной криптографии.
7. Однонаправленные функции.
8. Передача информации с использованием криптографии с открытыми ключами.
9. Цифровые подписи.
10. Протокол обмена ключами.
11. Удостоверение подлинности и обмен ключами.
12. Формальный анализ протоколов проверки подлинности и обмена ключами.
13. Криптографическая защита баз данных.
14. Промежуточные протоколы.
15. Электронная почта с подтверждением.
16. Безопасные вычисления с несколькими участниками.
17. Анонимная широковещательная передача сообщений.
18. Длинна симметричного и открытого ключа.
19. Управление ключами.

20. Типы алгоритмов.
21. Криптографические режимы.
22. Выбор алгоритма.
23. Шифрование коммуникационных каналов.
24. Шифрование хранимых данных.
25. Компрессия, кодирование и шифрование.
26. Скрытие шифртекста в шифртексте.
27. Теория информации.
28. Теория сложности.
29. Теория чисел.
30. Разложение на множители.
31. Генерация простого числа.
32. Дискретные логарифмы в конечном поле.
33. Стандарт шифрования данных DES.
34. Блочные шифры: LUCIFER, MADRYGA, REDOC, RC2, MMB.
35. Блочные шифры: ГОСТ, CAST, BLOWFISH, RC5.
36. Использование однонаправленных хэш-функций.
37. Объединение блочных шифров.
38. Однонаправленные хэш-функции: Snefru, N-хэш, MD4, MD5.
39. Алгоритм безопасного хэширования SHA.
40. Алгоритм цифровой подписи DSA.
41. Клеточные автоматы.
42. Преобразование схем идентификации в схемы подписи.
43. Криптография с несколькими открытыми ключами.
44. Неотрицаемые цифровые подписи.
45. Честные и отказоустойчивые криптосистемы.

## 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура оценивания знаний и умений состоит из следующих составных элементов: учета посещаемости лекционных занятий, подготовки конспектов, выполнения лабораторных работ, тестирования.

### Требования к выполнению лабораторных работ

Перед выполнением лабораторной работы требуется получить вариант задания. Далее необходимо ознакомиться с заданием. Выполнение лабораторной работы следует начать с изучения теоретических сведений, которые приводятся в соответствующих методических указаниях. Лабораторная работа считается выполненной, если: предоставлен отчет о результатах выполнения задания; проведена защита проделанной работы.

Защита работ проводится в два этапа: демонстрируются результаты выполнения задания, в случае лабораторной работы, предусматривающей разработку программного приложения при помощи тестового примера доказывается, что результат, получаемый при выполнении программы правильный, далее требуется ответить на ряд вопросов из перечня контрольных вопросов, который приводится в задании на работу.

Вариант задания выдается преподавателем, проводящим практические занятия. Отчет должен содержать следующие элементы: название работы, цель, задание, основную

часть, вывод по работе. Требования к оформлению и выполнению работы определены в методических рекомендациях.

**Требования к выполнению самостоятельных работ**

Целью выполнения самостоятельных работ (конспектов по тематике курса) является проработка соответствующих разделов курса посредством самостоятельного решения каждой задачи.

Конспект считается выполненным, если он предоставлен в соответствии с требованиями, является полным и имеет план. Требования к оформлению и выполнению работы определены в методических рекомендациях.

Промежуточная аттестация по дисциплине учитывает уровень результатов обучения, общее качество работы, самостоятельность. Освоение дисциплины оценивается по балльной шкале.

Общее количество баллов по дисциплине - 100 баллов.

Максимальное количество баллов, которое можно набрать в течение семестра за посещаемость, выполнение практических работ и самостоятельных работ, тестирование - 86 баллов.

За посещение лекционных занятий и написание конспектов магистрант может набрать максимально до 4 баллов.

За выполнение практических работ магистрант может набрать максимально 18 баллов (всего 6 лабораторных работ, по 3 балла за одну работу).

За выполнение самостоятельных работ магистрант может набрать максимально 24 балла (всего 8 конспектов, по 3 балла за один конспект).

За тестирование магистрант может набрать максимально 40 баллов (20 вопросов по 2 балла за один вопрос).

Обучающийся, набравший 41 балл и более, допускается к зачету. Максимальная сумма баллов, которые магистрант может набрать при сдаче зачета, составляет 14 баллов.

**Требования к зачету**

Для допуска к зачету по дисциплине необходимо выполнить все требуемые пункты отчетности. Существенным моментом является посещаемость занятий (в случае пропусков занятий предполагается более подробный опрос по темам пропущенных занятий). На зачет выносится материал, излагаемый в лекционном курсе и рассматриваемый на лабораторных занятиях. Для получения зачета необходимо правильно ответить на несколько поставленных вопросов. В затруднительных ситуациях (в отдельных случаях) допускается на зачете воспользоваться тетрадью с записью материалов лекций в присутствии преподавателя. При этом преподаватель может убедиться, в какой степени студент ориентируется в «своих» материалах, и по ряду дополнительных вопросов (по тетради).

**Структура оценивания зачета**

| Уровни оценивания | Критерии оценивания | Баллы |
|---|---|---|
| *оценка «отлично»* | Ставится, если студент обнаруживает всестороннее, систематическое и глубокое знание программного материала по дисциплине; обстоятельно анализирует структурную взаимосвязь рассматриваемых тем и разделов дисциплины; усвоил основную и знаком с дополнительной литературой, рекомендованной программой, а также усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии; проявил творческие способности в понимании, изложении и использовании учебного материала. | 14-12 |
| *оценка «хорошо»* | Ставится, если студент, обнаруживает полное знание программного материала, успешно выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; показал систематический характер знаний по дисциплине и способен к их самостоятельному пополнению и обновлению в ходе дальнейшей образовательной деятельности. | 11-9 |
| *оценка «удовлетворительно»* | Ставится, если студент обнаруживает знание основного программного материала в объеме, необходимом для дальнейшего обучения и профессиональной деятельности; справляется с выполнением заданий, предусмотренных программой; знаком с основной литературой, рекомендованной программой; допускает погрешности непринципиального характера в ответе на экзамене. | 8-6 |
| *оценка «неудовлетворительно»* | Ставится в том случае, если студент обнаруживает пробелы в знаниях основного программного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий. | 0-5 |