Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

УТВЕРЖДАЮ
Проректор
по учебно-методической работе
_____ А.А.Панфилов
«_17_» _____04_____ 20_15_г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ
(наименование дисциплины)

Направление подготовки 02.03.03 Математическое обеспечение и администрирование информационных систем

Профиль/программа подготовки:
Уровень высшего образования: бакалавриат
Форма обучения: очно-заочная (ускоренное обучение на базе СПО)

Семестр	Трудоемкость зач. ед,/ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
6	5/180	6	-	8	166	Зачет с оценкой
Итого	5/180	6	-	8	166	Зачет с оценкой

Владимир 20_15_

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины Безопасность информационных систем являются: изучение и практическое применение различных средств обеспечения безопасности и криптографических протоколов в современных информационных системах, а также знание методов устранения уязвимостей и программных ошибок в хранящихся в информационной системе данных.

Задачами дисциплины являются:

- изучение методов шифрования данных в информационных системах
- изучение криптографических протоколов и методов их функционирования
- изучение основных видов уязвимостей, влияющих на нормальное функционирование информационной системы.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Данная дисциплина относится к дисциплинам по выбору вариативной части ОПОП.

Изучение дисциплины происходит в 6 семестре и предполагает наличие у обучающихся фундаментальных знаний по информатике, теории чисел, знаний об устройстве и принципах функционирования компьютерных сетей и операционной системы, умение разрабатывать программы, на основе описания алгоритма, которые могут быть получены в рамках курсов «Основы программирования», «Архитектура вычислительных систем и компьютерных сетей», «Операционные системы и оболочки». Также необходимо знание основ языка C++, C#.

Знания полученные в рамках изучения дисциплины могут быть использованы при написании выпускной квалификационной работы, и в процессе профессиональной деятельности.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

В результате изучения дисциплины студент должен частично овладеть следующими компетенциями и продемонстрировать следующие результаты образования:

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения
ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно–коммуникационных технологий и с учётом основных требований информационной безопасности	*Знать:* основные требования к информационной безопасности в информационных системах, криптографические протоколы. *Уметь:* решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий с учётом требований информационной безопасности. *Владеть:* методами определения уязвимостей в информационных системах и библиографической и информационной культурой при решении стандартных профессиональных задач.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы,с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра)*, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
1	Информационные системы: виды и классификация.	6	1 - 18	2	-	-	-	30	-	- / -	Рейтинг-контроль №1. Защита лабораторных работ
2	Кодирование и шифрование данных в ИС	6			-	4	-	30	-	2 / 50%	
3	Криптографические протоколы безопасности в ИС	6		2	-	2	-	52	-	2 / 50%	Рейтинг-контроль №2. Защита лабораторных работ
4	Методы обеспечения безопасности ИС	6		2		2		54		- / -	Рейтинг-контроль №3. Защита лабораторных работ
Итого				6		8	-	166		4 / 29%	Зачет с оценкой

Тематика лекционных занятий

Раздел 1. Информационные системы: виды и классификация.

1. Понятие информационной системы. Структурный состав элементов информационной системы.
2. Виды информационных систем и их классификация.

Раздел 2. Кодирование и шифрование данных в ИС.

1. Понятие кодирования и шифрования данных. Алгоритмы шифрования.
2. Симметричные и асимметричные алгоритмы. Блочные шифры.
3. Понятие криптоанализа данных: виды криптоанализа.
4. Основные виды атак на данные в ИС.

Раздел 3. Криптографические протоколы безопасности в ИС.

1. Понятие криптобезопасности ИС. Протоколы шифрования данных.
2. Уровни обеспечения безопасности данных в ИС.
3. Технические средства и программные продукты для обеспечения безопасности данных.

Раздел 4. Методы обеспечения безопасности данных в ИС.

1. Модель уязвимой среды Долева-Яо. Классификация и характеристики угроз безопасности данных.
2. Методы обеспечения безопасности данных в ИС.

Тематика лабораторных занятий

1. Изучение методов кодирования данных.
2. Алгоритм шифрования данных SHA-5.
3. Блочные шифры.
4. Стеганография данных.
5. Одноразовый блокнот.
6. Криптографические протоколы.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В данной дисциплине применяются следующие образовательные технологии:

- лекционно-семинарская система обучения (традиционные лекционные и лабораторные занятия);
- разбор ситуаций при обнаружении уязвимости информационной системы;
- технология развития критического мышления (прививание студентам навыков критической оценки разработанных ими алгоритмов);
- мультимедиа-технологии (проведение лекционных и лабораторных занятий с использованием проекторов и других мультимедийных устройств).
- метод (case-study) студенты получают «проблемные» задания по тематике изучаемого раздела.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Контроль усвоения материала студентами проводится в форме письменных контрольных работ по разделам дисциплины и защиты лабораторных работ. По итогам изучения дисциплины проводится зачет с оценкой.

Для каждой контрольной работы составляются билеты, содержащие 2 вопроса из предложенных ниже перечней.

А. Вопросы для рейтинг-контроля.

Вопросы для рейтинг-контроля№1.

1. Понятие и виды ИС.
2. Характеристика ИС.
3. Уровни безопасности ИС.
4. Участники информационного процесса: их роли и функции.
5. Права и правила доступа к информации.
6. Стандарты безопасности для ИС.
7. Структура данных в ИС.
8. Стандарты информационной безопасности в России.
9. Понятие доверенной системы.
10. Понятие безопасной системы.
11. Монитор обращений и его качества.
12. Ядро безопасности монитора обращений.
13. Политика безопасности.
14. Периметр безопасности.
15. Канал утечек.
16. Угрозы: виды и классификация.

Вопросы для рейтинг-контроля№2.

1. Понятие криптографии.
2. Шифрование и кодирование данных.
3. Классы безопасности.
4. Класс безопасности С1 и его характеристика.
5. Простые перестановочные шифры.
6. Симметричные и асимметричные алгоритмы шифрования.
7. Класс безопасности С2 и его характеристика.
8. Алгоритм шифрования с открытым ключом.
9. Пространство ключей.
10. Класс В1 и его характеристика.

11. Класс B2: характеристика.
12. Класс B3: характеристика.
13. Класс A: характреристика.
14. Криптоанализ: понятие и виды.
15. Дешифрование данных.
16. Криптостойкость алгоритма.
17. Абсолютно стойкие системы.
18. Достаточно стойкие системы.
19. Расчёт трудоёмкости алгоритма.
20. Кодирование данных с использованием шифра Цезаря.
21. Кодирование данных с использованием шифра Виженера.
22. Кодирование данных с использованием шифра ДНК.

Вопросы для рейтинг-контроля№3.

1. Понятие и виды ЭЦП.
2. Криптографические протоколы и их виды.
3. Самоутверждающийся криптографический протокол.
4. Протокол с посредником.
5. Кодирование данных с использованием шифра ДНК.
6. Самодостаточные протоколы.
7. Методы вскрытия протоколов.
8. Оценка криптостойкости систем шифрования данных.
9. Кодирование данных с частью ключа с помощью шифра Виженера.
10. Принцип Керкгоффса и его требования к алгоритму шифрования данных.
11. Виды шифротекста.
12. Дифференциальный метод криптоанализа.
13. Линейный метод криптоанализа.
14. Поточные и блочные алгоритмы шифрования данных: характеристика.
15. Классификация блочных шифров.
16. Методы защиты данных в ИС.
17. Двойное шифрование.
18. Классификация поточных шифров.
19. СПШ: понятие,характеристика.
20. АПШ:понятие, харктеристика.
21. Классификация алгоритмов ЭЦП.

Б. Лабораторные работы

Каждая лабораторная работа проверяется на корректность работы и защищается в форме опроса по сделанной работе.

По каждой лабораторной работе может быть задан по коду программы, например, пояснить назначение фрагмента кода, как реализован алгоритм, обосновать выбор типов данных и подходов к реализации алгоритма.

Остальные вопросы приведены ниже:

1. Изучение методов кодирования данных.
    1. Расчёт трудоёмкости алгоритма.
    2. Классификация видов шрифта.
    3. Что такое идентификация?
    4. Что такое аутентификация?
    5. Поясните общую идею шифра с симметричным шрифтом.
    6. Поясните отличия между шифром подстановки и шифром перестановки.
    7. Поясните отличия между моноалфавитным и многоалфавитным шифрами.
    8. Поясните отличия между шифром потока и блочным шифром.
    9. Все ли шифры потока являются моноалфавитными? Поясните.
    10. Все ли блочные шифры являются многоалфавитными? Поясните.

11. Перечислите три моноалфавитных шифра.
12. Перечислите три многоалфавитных шифра.
13. Перечислите два шифра перестановки.
14. Перечислите четыре вида атак криптоанализа.

2. Алгоритм шифрования данных SHA-5.
1. Что такое хэш-код?
2. Длина хэш-кода.
3. Применение хэш-кодирования.
4. Криптостойкость алгоритмов.
5. Приведите примеры реальных ситуаций, требующих хэш-код.

3. Блочные шифры.
1. К какому классу шрифтов относится алгоритм RC4?
2. Охарактеризуйте криптостойкость алгоритма.
3.Расскажите суть алгоритма.
4.Приведите примеры блочных шифров.

4. Стеганография данных.
1. Что такое стеганография?
2. Приведите примеры практического применения стеганографии.
3. Алгоритм преобразования графического изображения JPEG.
4. Криптостойкость алгоритма.

5. Одноразовый блокнот.
1. Опишите реализацию алгоритма.
2. Коммерциализация алгоритма.
3. Возможность массового использования.
4. Криптостойкость алгоритма.

6. Криптографические протоколы.
1. В чем суть модели Долева –Яо.
2. Что такое протокол?
3. Кто может выступать в качестве участников протокола?
4. Как характеризуется цикл протокола?
5. Что такое сеанс?
6. Коммуникационный протокол – это?
7. Перечислите функции-сервисы безопасности.
8. Перечислите свойства, характеризующие безопасность протоколов.

В. Вопросы к зачету с оценкой

1. Понятие информационной системы: классификация и разновидности.
2. Информационная безопасность: основные понятия.
3. Алгоритмы шифрования данных в ИС: симметричные и асимметричные.
4. Симметричный алгоритм шифрования данных: методика шифрования, применение в ИС.
5. Асимметричный алгоритм шифрования данных.
6. Криптоанализ: понятие, разновидности, основные методы.
7. Уровни безопасности данных в ИС.
8. Участники информационного процесса: роли и функции.
9. Угрозы безопасности данных: виды и классификация.
10. Блочные шифры: виды, методика шифрования, виды атаки.
11. Поточные шифры: методика шифрования.
12. Шифр «одноразовый» блокнот: методика шифрования данных, криптостойкость.
13. Шифр XOR: алгоритм работы, применение при кодировании данных.
14. ЭЦП: понятие, виды и применение при шифровании данных в ИС.

15. Простые перестановочные шифры: понятие, виды перестановок, применение при кодировании данных.
16. Шифр Виженера: методика шифрования и дешифрования данных.
17. Шифр Цезаря: методика шифрования и дешифрования данных.
18. Шифр AES: методика шифрования данных.
19. Нормативно-правовые основы обеспечения безопасности данных в ИС.
20. Несанкционированный доступ: понятие, виды, оценка степени угрозы безопасности данных в ИС.
21. Права и правила доступа к данным в ИС.
22. Стеганография: понятие, виды, применение при шифровании данных.
23. Квантовая криптография: понятие, методика кодирования, применение в ИС.
24. Квантовый криптоанализ: виды атаки на данные в ИС.
25. Хзш-таблицы: применение при кодировании данных.
26. Сеть Фейстеля: методика кодирования данных, применение в ИС.
27. Кодовые деревья: структура, виды, классификация.
28. Энтропия: понятие, методика расчёта, применение в шифровании данных.
29. Гаммирование: понятие, способы расчёта, применение в кодировании информации.
30. Технические средства для обеспечения безопасности данных в ИС.
31. Вирусы: виды, классификация.
32. Вредоносные воздействия: понятие, виды, методы воздействия на информацию.
33. Криптографические протоколы: виды и классификация.
34. Методы защиты данных в ИС.
35. Простые подстановочные шифры: понятие, виды подстановок, применение при кодированиии данных.
36. Алгоритм Евклида: понятие, модификации, применение при шифровании данных.
37. Криптосистема: виды и структура.
38. Алгоритмы ГОСТ: методика шифрования и практическое использование.
39. Конфиденциальная информация: понятие, виды.
40. КИС: понятие, характеристика структурных элементов.

Б. Самостоятельная работа

Самостоятельная работа по дисциплине представлена в нескольких видах:

А) изучение теоретического материала для подготовки к зачету (литературные источники);

Б) решение практических задач по определению уязвимостей информационных систем (разработка программ).

Порядок выполнения самостоятельной работы следующий: все задания вида А проверяются в процессе сдачи зачета; задания группы Б предусматривают несколько уровней оценки: (оптимизация программного кода, интерфейс программы (консольное или оконное приложение), уровень владения языком программирования). Все перечисленные параметры заданий группы Б учитываются в качестве допуска к сдаче зачета и предоставляются на бонусных баллов в итоговой оценке обучающегося.

Особое внимание нужно уделить следующим разделам дисциплины:**1. Кодирование и шифрование данных в ИС, 2. Криптографические протоколы безопасности, 3. Методы обеспечения безопасности данных в ИС.** Данные разделы дисциплины формируют у обучающихся практические навыки кодирования и шифрования информации и понятийный аппарат по изучаемой тематике.

Вопросы для контроля самостоятельной работы:

Раздел №1.

17. Понятие и виды ИС.
18. Характеристика ИС.
19. Уровни безопасности ИС.
20. Участники информационного процесса: их роли и функции.
21. Права и правила доступа к информации.
22. Стандарты безопасности для ИС.
23. Структура данных в ИС.
24. Стандарты информационной безопасности в России.
25. Понятие доверенной системы.
26. Понятие безопасной системы.
27. Монитор обращений и его качества.
28. Ядро безопасности монитора обращений.
29. Политика безопасности.
30. Периметр безопасности.
31. Канал утечек.
32. Угрозы: виды и классификация.

Раздел №2.

23. Понятие криптографии.
24. Шифрование и кодирование данных.
25. Классы безопасности.
26. Класс безопасности С1 и его характеристика.
27. Простые перестановочные шифры.
28. Симметричные и асимметричные алгоритмы шифрования.
29. Класс безопасности С2 и его характеристика.
30. Алгоритм шифрования с открытым ключом.
31. Пространство ключей.
32. Класс В1 и его характеристика.
33. Класс В2: характеристика.
34. Класс В3: характеристика.
35. Класс А: характеристика.
36. Криптоанализ: понятие и виды.
37. Дешифрование данных.
38. Криптостойкость алгоритма.
39. Абсолютно стойкие системы.
40. Достаточно стойкие системы.
41. Расчёт трудоёмкости алгоритма.
42. Основные свойства защищаемой информации.
43. В чём отличие алгоритма Виженера от алгоритма Цезаря.
44. Что называется афинной перестановкой.
45. Кодирование данных с использованием шифра Цезаря.
46. Кодирование данных с использованием шифра Виженера.
47. Кодирование данных с использованием шифра ДНК.
48. Понятие и виды ЭЦП.
49. Криптографические протоколы и их виды.
50. Самоутверждающийся криптографический протокол.
51. Протокол с посредником.
52. Кодирование данных с использованием шифра ДНК.
53. Самодостаточные протоколы.
54. Методы вскрытия протоколов.
55. Оценка криптостойкости систем шифрования данных.
56. Кодирование данных с частью ключа с помощью шифра Виженера.
57. Принцип Керкгоффса и его требования к алгоритму шифрования данных.

58. Виды шифротекста.
59. Дифференциальный метод криптоанализа.
60. Линейный метод криптоанализа.
61. Поточные и блочные алгоритмы шифрования данных: характеристика.
62. Классификация блочных шифров.
63. Методы защиты данных в ИС.
64. Двойное шифрование.
65. Классификация поточных шифров.
66. СПШ: понятие,характеристика.
67. АПШ:понятие, характеристика.
68. Классификация алгоритмов ЭЦП.
69. В чём преимущества метода шифрования данных: «одноразовый блокнот».
70. Что называется объектом защиты.
71. Как осуществляется шифрование данных в алгоритме AES.
72. В чем суть метода шифрования данных с помощью хэш-таблиц.
73. В чём состоит метод шифрования данных с помощью блоков.
74. Как проверить, достоверна ли переданная информация.
75. Что называется контрольным битом в сообщении.
76. Какова взаимосвязь между субъектом, предметом и объектом защиты.
77. Что называется бандитским криптоанализом.
78. Что представляет собой уязвимая среда в модели Долева-Яо.

Раздел №3.

22. Понятие и виды ЭЦП.
23. Криптографические протоколы и их виды.
24. Самоутверждающийся криптографический протокол.
25. Протокол с посредником.
26. Кодирование данных с использованием шифра ДНК.
27. Самодостаточные протоколы.
28. Методы вскрытия протоколов.
29. Оценка криптостойкости систем шифрования данных.
30. Кодирование данных с частью ключа с помощью шифра Виженера.
31. Принцип Керкгоффса и его требования к алгоритму шифрования данных.
32. Виды шифротекста.
33. Дифференциальный метод криптоанализа.
34. Линейный метод криптоанализа.
35. Поточные и блочные алгоритмы шифрования данных: характеристика.
36. Классификация блочных шифров.

Раздел №4.

1. Криптосистема: виды и структура.
2. Алгоритмы ГОСТ: методика шифрования и практическое использование.
3. Конфиденциальная информация: понятие, виды.
4. КИС: понятие, характеристика структурных элементов.
5. Методы защиты данных в ИС.
6. Двойное шифрование.
7. Классификация поточных шифров.
8. СПШ: понятие,характеристика.
9. АПШ:понятие, харктеристика.
10. Классификация алгоритмов ЭЦП.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

а) основная литература:

1.Оценка относительного ущерба безопасности информационной системы: Монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 192 с.: ил.; 60x88 1/16 + 11 с.. - (Научная мысль). (о) ISBN 978-5-369-01371-7 (ЭБС ЗНАНИУМ)

2. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5, 1000 экз.(ЭБС ЗНАНИУМ).

3. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; 70x100 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4 (ЭБС ЗНАНИУМ).

б) дополнительная литература:

1. Агапов, А. В. Обработка и обеспечение безопасности электронных данных [Электронный ресурс] : учеб.пособие / А. В. Агапов, Т. В. Алексеева, А. В. Васильев и др.; под ред. Д. В. Денисова. - М.: МФПУ Синергия, 2012. - 592 с. - (Сдаем госэкзамен). - ISBN 978-5-4257-0074-2. (ЭБС ЗНАНИУМ).

2. Монахов, Ю. М.Функциональная устойчивость информационных систем : учебное пособие : в 3 ч. / Ю. М. Монахов ; Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых (ВлГУ) .— Владимир : Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых (ВлГУ), 2011- .— (Комплексная защита объектов информатизации ; кн. 22) .Ч. 1: Надежность программного обеспечения [Электронный ресурс] .— Электронные текстовые данные (1 файл: 560 Кб) .— 2011 .— 60 с. : ил. — Заглавие с титула экрана .— Электронная версия печатной публикации .— Библиогр.: с. 53-57 .— Свободный доступ в электронных читальных залах библиотеки (Внутривузовские издания ВлГУ http://e.lib.vlsu.ru:80/handle/123456789/2972.)

3.Золотарев, В. В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб.пособие/ В. В. Золотарев, Е. А. Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с.(ЭБС ЗНАНИУМ).

в) периодические издания

1. Информационная безопасность. Архив номеров. // Режим доступа: http://www.infosecurityrussia.ru/2015/itsec

2. Технологии защиты. Архив номеров. //Режим доступа: http://www.tzmagazine.ru/

3. SecurityNews. Архив номеров.//Режим доступа: http://www.secnews.ru/

в) интернет-ресурсы

1. Информационная безопасность // Режим доступа: http://protect.htmlweb.ru/p01.htm

2. Система информационной безопасности //Режим доступа: http://tvoi.biz/biznes/informatsionnaya-bezopasnost/sistema-informatsionnoj-bezopasnosti.html

3. Владимир Липаев. Основные факторы, определяющие технологическую безопасность информационных систем // Режим доступа: http://www.computer-museum.ru/histsoft/ji97061.htm.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

В качестве материально-технического обеспечения дисциплины используются следующие средства: проектор, наборы слайдов по учебной тематике, компьютерные классы с установленным ПО: VS 2012, 2013,2015, мультимедийные аудитории.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 02.03.03 Математическое обеспечение и администрирование информационных систем

Рабочую программу составил ст. преподаватель кафедры ФиПМ Павлова О.Н.
(ФИО, подпись)

Рецензент
(представитель работодателя) ген. директор ООО "РСервис" Квасов Д.С.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ФиПМ
Протокол № 11А от 17.04.15 года
Заведующий кафедрой _____ Аракелян С.М.
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 02.03.03 Математическое обеспечение и администрирование информационных систем
Протокол № 11А от 17.04.15 года
Председатель комиссии _____ Аракелян С.М.
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на _____ учебный год
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой _____

Рабочая программа одобрена на _____ учебный год
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой _____

Рабочая программа одобрена на _____ учебный год
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой _____