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 2015 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ

(наименование дисциплины)

Направление подготовки 02.03.03Математическое 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	18	-	36	126	Зачет с оценкой
Итого	5/180	18	-	36	126	Зачет с оценкой

Владимир 2015

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины Защита информации являются: изучение основных методов и способов защиты информации; современных криптографических алгоритмов; устранение и предотвращения несанкционированного доступа в систему.

Задачами дисциплины являются:

- изучение методов шифрования информации
- изучение методов и способов защиты информации
- изучение современных криптографических алгоритмов.

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», «Алгебра и теория чисел», «Структуры и алгоритмы компьютерной обработки данных», «Архитектура вычислительных систем и компьютерных сетей», «Операционные системы и оболочки». Также необходимо знание основ языка C++, C#.

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 способы кодирования и шифрования информации; методы и способы защиты информации; современные криптографические алгоритмы. *Уметь:* решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности. *Владеть:* информационной и библиографической культурой применения информационно-коммуникационных технологий при кодировании информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ п/п	Раздел (тема)	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)	Объем учебной работы,с применением интерактивных	Формы текущего контроля успеваемости *(по неделям*

	дисциплины			Лекции	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР	методов (в часах / %)	семестра), форма промежуточной аттестации (по семестрам)
1	Концептуальные основы защиты информации	6	1-18	4	-	-	-	20	-	- / -	Рейтинг-контроль №1
2	Основные методы и способы защиты информации	6		8	-	24	-	64	-	8 / 25%	Рейтинг-контроль №2. Защита лабораторных работ
3	Современные криптографические алгоритмы и области их применения	6		6	-	12	-	42	-	9 / 50%	Рейтинг-контроль №3. Защита лабораторных работ
Итого				18		36	-	126		17 / 31%	Зачет с оценкой

Тематика лекционных занятий

Раздел 1. Концептуальные основы защиты информации.

1. Основные понятия защиты информации. Участники информационного процесса. Процедура идентификации, аутентификации, авторизации пользователя.

Раздел 2. Основные методы и способы защиты информации.

1. Понятие кодирования и шифрования данных. Алгоритмы шифрования.
2. Симметричные и асимметричные алгоритмы. Блочные шифры.
3. Понятие криптоанализа данных: виды криптоанализа.
4. Цифровая подпись, хэш-код.
5. Модель уязвимой среды Долева-Яо.

Раздел 3. Современные криптографические алгоритмы и области их применения.

1. Стеганография: виды и методы. Шифр DES, AES.
2. Квантовая криптография и криптоанализ.

Тематика лабораторных занятий

1. Изучение методов кодирования данных.
2. Шифр Виженера.
3. Одноразовый блокнот.
4. Алгоритм RC4.
5. Алгоритм SHA или MD5.
6. Шифр DES.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В данной дисциплине применяются следующие образовательные технологии:

- лекционно-семинарская система обучения (традиционные лекционные и лабораторные занятия);
- метод проектов (разработка и реализация на лабораторных работах основных этапов жизненного цикла проекта – анализ, проектирование, разработка и реализация решения задачи);
- 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 контрольных работ по разделам курса и защиты лабораторных работ.

А. 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. Шифр Виженера.
   1. В чём отличие алгоритма Виженера от алгоритма Цезаря
   2. Расскажите суть алгоритма.
   3. Охарактеризуйте криптостойкость алгоритма.
   4. .Алгоритм декодирования шифра Виженера.
3. Одноразовый блокнот.
   1. Опишите реализацию алгоритма.
   2. Коммерциализация алгоритма.
   3. Возможность массового использования.
   4. Криптостойкость алгоритма.
4. Алгоритм RC4.
   1. К какому классу шрифтов относится?
   2. Охарактеризуйте криптостойкость алгоритма.
   3.Расскажите суть алгоритма.
5. Алгоритм SHA или MD5.
   1. Что такое хэш-код?
   2. Длина хэш-кода.
   3. Применение хэш-кодирования.
   4. Криптостойкость алгоритмов.
   5. Приведите примеры реальных ситуаций, требующих хэш-код.

6. Шифр AES.

1. Количество раундов обработки алгоритма.
2. Величина блока обработки входного сообщения.
3.Безопасность алгоритма.
4. Перечислите параметры (размер блока, размер ключа и число раундов) для трех версий AES.
5. Сколько преобразований имеется в каждой версии AES? Сколько ключей необходимо для каждой версии?
6. Сравните DES и AES. Какой из них ориентирован на работу с битом, а какой — на работу с байтом?
7. Определите матрицу состояний в AES. Сколько матриц состояний имеется в каждой версии AES?
8. Какие из четырех преобразований, определенных для AES, изменяют содержание байтов, а какие — не изменяют?
9. Сравните подстановку в DES и AES. Почему мы имеем только одну таблицу перестановки (S -блок) в AES и несколько — в DES?
10. Сравните перестановки в DES и AES. Почему надо иметь расширение и сжатие перестановки в DES и не надо — в AES?
11. Сравните ключи раунда в DES и AES. В каком шифре размер ключа раунда равен размеру блока?
12. Почему смешивающее преобразование (MixColumns) нужно в DES, но не нужно в AES?

Б. Вопросы рейтинг-контроля

Вопросы для рейтинг-контроля№1.

1. Понятие защиты информации.
2. Свойства информации.
3. Участники информационного процесса: их роли и функции.
4. Права и правила доступа к информации.
5. Стандарты безопасности для ИС.
6. Структура данных в ИС.
7. Стандарты информационной безопасности в России.
8. Угрозы: виды и классификация.
9. Дешифровать шифротекст с использованием шифра Цезаря: «Kphrtocvkqpeqfgkuxgtaukosngogwjqfqhxkuwcnkucvkqp»
10. Раскодировать следующую строку сообщения, используя код Цезаря: «Oljkw#vljqdo#lv#d#rqh#ri#pdqb#wbshv#ri#vljdov» (# означает пробел)
11. Дайте определение понятию «информационный объект»
12. Виды криптоанализа: характеристика.
13. Адаптивное вскрытие с открытым шифротекстом.
14. Вскрытие с использованием открытого текста.
15. Дайте определение понятию «безопасность информационного объекта».
16. Алгоритм с открытым ключом.
17. Алгоритм с закрытым ключом.
18. Симметричная криптосистема.
19. Асимметричная криптосистема.

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 В2: характеристика.
12. Класс В3: характеристика.
13. Класс А: 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, характеристика.
21. Классификация алгоритмов ЭЦП.

В. Вопросы к зачету с оценкой

1. Понятие информационной системы: классификация и разновидности.
2. Защита информации: 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. Алгоритм RC4: методика шифрования данных.
8. Участники информационного процесса: роли и функции.
9. Угрозы безопасности информации: 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. Правовое обеспечение защиты информации.
20. Несанкционированный доступ: понятие, виды, оценка степени угрозы безопасности данных в ИС.
21. Права и правила доступа к информации.
22. Стеганография: понятие, виды, применение при шифровании данных.
23. Квантовая криптография: понятие, методика кодирования.
24. Квантовый криптоанализ: виды атаки на данные.
25. Хэш-таблицы: применение при кодировании данных.
26. Сеть Фейстеля: методика кодирования данных.
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. Использование СТЕЛС технологий в вирусных программах.
31. Вирусы:виды, классификация.
32. Вредоносные воздействия: понятие, виды, методы воздействия на информацию.
33. Криптографические протоколы: виды и классификация.
34. Система с открытым ключом Диффи-Хеллмана.
35. Простые подстановочные шифры: понятие, виды подстановок, применение при кодировании 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.
41. Генераторы псевдослучайных чисел.
42. Информационные системы, сети, каналы и среды.
43. Организационно-административные методы защиты информации.

Г. Самостоятельная работа

Самостоятельная работа по дисциплине представлена в нескольких видах:

А) изучение теоретического материала для подготовки к рейтингу и экзамену (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 итоговом рейтинге обучающегося.

Особое внимание нужно уделить следующим разделам дисциплины:**1. Основные методы и способы защиты информации, 2. Современные криптографические алгоритмы и области их применения.** 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.

20. Понятие защиты информации.
21. Свойства информации.
22. Участники информационного процесса: их роли и функции.
23. Права и правила доступа к информации.
24. Стандарты безопасности для ИС.
25. Структура данных в ИС.
26. Стандарты информационной безопасности в России.
27. Угрозы: виды и классификация.
28. Что называется НОД и сфера его применения при шифровании данных.
29. Что называется криптостойкостью алгоритма шифрования данных.
30. В чём отличие адаптивного вскрытия от вскрытия с открытым шифротекстом.
31. В чем отличие прав доступа от правил доступа к данным.
32. Как рассчитать энтропию информационной системы.
33.
34. Дешифровать шифротекст с использованием шифра Цезаря: «Kphrtocvkqpeqfgkuxgtaukosngogwjqfqhxkuwcnkucvkqp»
35. Раскодировать следующую строку сообщения, используя код Цезаря: «Oljkw#vljqdo#lv#d#rqh#ri#pdqb#wbshv#ri#vljdov» (# означает пробел)
36. Дайте определение понятию «информационный объект»
37. Виды криптоанализа: характеристика.
38. Адаптивное вскрытие с открытым шифротекстом.
39. Вскрытие с использованием открытого текста.
40. Дайте определение понятию «безопасность информационного объекта».
41. Алгоритм с открытым ключом.
42. Алгоритм с закрытым ключом.
43. Симметричная криптосистема.
44. Асимметричная криптосистема.

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.

1. Методы сокрытия информации с помощью стеганографии.
2. Атаки на поточные шифры.
3. Что называется СПШ.
4. Виды атаки на блочные шифры.
5. Угрозы безопасности.
6. Что называется доступностью данных.
7. В чём отличие симметричного алгоритма от асимметричного.
8. В чем суть метода коллизий при криптоанализе данных.
9. Как определить подлинность ЭЦП.
10. Что представляет собой метод «радужных» таблиц в криптоанализе.
11. Как осуществляется вскрытие по методу «дат» рождения.
12. Каковы основные условия для обеспечения безопасности данных в ИС.
13. В чём суть метода криптоанализа: «атака грубой силой».
14. Что называется однофакторной и многофакторной защитой данных. В чём преимущества одной над другой.
15. Чем отличается уязвимость системы от неисправностей в ней.
16. В чём суть метода гаммирования данных.

17. В чём суть алгоритма Луна.
18. DDOS –атака,как вид угрозы информационной безопасности.
19. Программные закладки и их влияние на безопасность информации.

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

а) основная литература:

1.Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6, 500 экз. (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. Методы и средства защиты информации [Электронный ресурс]: методические указания к лабораторным работам / С. В. Маскеев, М. А. Трофимов; Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых (ВлГУ), Кафедра вычислительной техники .— Электронные текстовые данные (1 файл: 317 Кб) .— Владимир : Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых (ВлГУ), 2013 .— 19 с. : ил. — Заглавие с титула экрана.— Электронная версия печатной публикации .— Библиогр.: с. 18 .— Свободный доступ в электронных читальных залах библиотеки.(ВнутривузовскиеизданияВлГУhttp://e.lib.vlsu.ru/bitstream/123456789/3325/1/01254.pdf>)

б) дополнительная литература:

1.Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с.: 60x88 1/8. - (Высшее образование: Бакалавриат). (обложка) ISBN 978-5-369-01304-5, 200 экз.(ЭБС ЗНАНИУМ).

2. 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).

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) _____
(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 _____