МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского»

Механико-математический факультет

УТВЕРЖДАЮ
Проректор по учебно-методической работе
д.ф.н., профессор _____ Е.Г. Елина
"__" _____ 2016 г.

Рабочая программа дисциплины

Математические основы информационной безопасности

Направление подготовки бакалавриата
38.03.05 – Бизнес-информатика
Профиль подготовки – Управление бизнес процессами

Квалификация (степень) выпускника
Бакалавр

Форма обучения
очная

Саратов,
2016 год

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Саратовский национальный исследовательский государственный
университет имени Н.Г. Чернышевского»

Механико-математический факультет

УТВЕРЖДАЮ
Проректор по учебно-методической работе
д.ф.н., профессор _____Е.Г. Елина
"__"_____2016 г.

Рабочая программа дисциплины

Математические основы информационной безопасности

Направление подготовки бакалавриата
38.03.05 – Бизнес-информатика
Профиль подготовки – Управление бизнес процессами

Квалификация (степень) выпускника
Бакалавр

Форма обучения
очная

Саратов,
2016 год

1. Цели освоения дисциплины

Цели освоения дисциплины «Математические основы информационной безопасности» заключаются в получении представления о современной методологии обеспечения информационной безопасности и о роли математических методов и программно-технических средств в обеспечении информационной безопасности, в подготовке к применению методов обеспечения информационной безопасности на этапах проектирования, разработки и эксплуатации сложно организованных программных систем.

2.Место дисциплины в структуре ООП

Дисциплина Б1.Б.18 «Математические основы информационной безопасности» является базовой дисциплиной блока «Дисциплины» Федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению 38.03.05 «Бизнес-информатика» (бакалавриат).

Изучение дисциплины «Математические основы информационной безопасности» основывается на базе знаний, полученных студентами в ходе освоения дисциплин «Информационные системы и технологии» и «Дискретная математика» базовой части, а также дисциплин «Информатика и программирование» и «Введение в математику и информатику» вариативной части ФГОС ВО.

Дисциплина «Математические основы информационной безопасности» изучается на четвертом году обучения и является одной из важнейших терминальных дисциплин, завершающих базовую подготовку бакалавра бизнес-информатики.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В совокупности с другими дисциплинами ФГОС ВО дисциплина «Математические основы информационной безопасности» обеспечивает инструментарий формирования следующих общекультурных компетенций бакалавра бизнес-информатики:

ОК-7 – способность к самоорганизации и самообразованию

В совокупности с другими дисциплинами ФГОС ВО дисциплина «Математические основы информационной безопасности» обеспечивает инструментарий формирования следующих общепрофессиональных компетенций бакалавра бизнес-информатики:

ОПК-1 – способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ОПК-3 – способность работать с компьютером как средством управления информацией, работать с информацией из различных источников, в том числе в глобальных компьютерных сетях.

В результате освоения содержания дисциплины «Математические основы информационной безопасности» студент должен:

знать

- математические основы, необходимые для решения задач обеспечения информационной безопасности;
- основные криптографические методы, алгоритмы и протоколы;
- основные положения методологии комплексного подхода к обеспечению информационной безопасности;
- виды угроз ИС и методы обеспечения информационной безопасности;
- типовые математические модели информационно безопасных систем;
- основные программно-технические методы и средства обеспечения информационной безопасности подконтрольных объектов, их роль и место в программной архитектуре компьютерных систем;
- типовые подходы к программной реализации базовых сервисов безопасности в компьютерных системах;
- типовые ошибки программирования, приводящие к уязвимостям компьютерных систем;

уметь

- применять математические методы в обеспечении информационной безопасности;
- проводить анализ защищенности информационной системы, разрабатывать модели угроз для информационной системы, проектировать и внедрять систему защиты информации в соответствии с разработанной моделью угроз;
- использовать специализированное программное обеспечение для решения задач информационной безопасности;
- выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС;

владеть

- понятийным аппаратом информационной безопасности;

- навыками применения современного математического инструментария для решения задач в сфере информационной безопасности;

- методикой построения, анализа и применения математических моделей для оценки степени защищенности информационной системы, качества использованных алгоритмов и технологий;

- навыками применения положений современных нормативных документов и стандартов в области информационной безопасности;

- навыками проведения аудита программного обеспечения на предмет наличия типовых ошибок программирования.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 часов).

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости *(по неделям семестра)* Формы промежуточной аттестации *(по семестрам)*
				Лекции	Лаб.	Прак. занятия	КСР	СРС	
1.	Основные понятия информационной безопасности	7	1-2	2	4				
2.	Элементы теории информации и кодирования.	7	3-6	4	4			4	
3.	Математические основы криптографии	7	7-10	4	12			4	
4.	Криптографические методы защиты информации.	7	11-16	6	12			4	
5.	Идентификация и аутентификация.	7	17-18	2	4		2	4	к.р.
	Всего в 7 семестре			**18**	**36**		**2**	**16**	**Зачет**
6.	Протоколирование и аудит.	8	1-2	1	2			4	
7.	Компьютерные вирусы.	8	3-4	2	2			4	
8.	Средства защиты сети.	8	5-6	2	2			4	
9.	Средства и методы противодействия угрозам доступности информации.	8	7-8	2	2			4	
10.	Основные принципы построения систем защиты.	8	9-10	2	2			6	
11.	Информационная безопасность с точки зрения технологии программирования.	8	11-12	2	2		2	5	
12.	Техника и методология атаки.	8	13-14	2	1			4	к.р.
	Всего в 8 семестре			**13**	**26**		**2**	**31**	**Экз. 36**
	Итого:			**31**	**62**		**4**	**47**	**36**

Содержание разделов дисциплины

Раздел 1. Основные понятия информационной безопасности

1.1. Предмет информационной безопасности. Свойства компьютерной информации, важные с точки зрения информационной безопасности: конфиденциальность, целостность и доступность.

1.2. Угрозы информационной безопасности.

1.3. Каналы утечки информации.

1.4. Неформальная модель нарушителя.

1.5. Обзор стандартов и нормативно-правовой базы в сфере информационной безопасности.

Раздел 2. Элементы теории информации и кодирования

2.1. Сигналы, данные и методы получения информации. Свойства информации.

2.2. Количество информации как мера уменьшения неопределенности знаний. Алфавитный подход к вычислению количества информации.

2.3. Определение вероятности и основные правила вычисления количества информации.

2.4. Информационная модель Шеннона.

2.5. Формулы Шеннона и Хартли.

2.6. Понятие кода. Связь между информационной емкостью и средней длиной кода. Избыточность кодирования.

2.7. Метод сжатия по Хаффману. Код Хэмминга

Раздел 3. Математические основы криптографии

3.1. Множества и отношения. Бинарные отображения.

3.2. Основная теорема арифметики. Алгоритм деления в Z.

3.3. Понятие группы. Изоморфизмы групп.

3.4. Понятие и свойства колец. Кольцо вычетов.

3.5. Понятие поля. Поля Галуа.

3.6. Кольца многочленов. Алгоритм деления в A[X]. Разложение в кольце многочленов. Неприводимые многочлены.

3.7. Китайская теорема об остатках

3.8. Эллиптические кривые.

Раздел 4. Криптографические методы защиты информации

4.1. Понятие симметричных алгоритмов шифрования.

4.2. Обзор классических симметричных алгоритмов. Моноафавитный шифр. Шифр Гронсфельда. Шифр Плейфейера. Шифр Хилла. Одноразовый блокнот. Перестановочные шифры.

4.3. Диффузия и коффузия. Схема Файстеля.

4.4. Обзор современных симметричных алгоритмов шифрования. Шифр DES. Шифр AES.

4.5. Режимы функционирования блочных шифров.

4.6. Скремблеры.

4.7. Виды криптоанализа симметричных алгоритмов.

4.8. Шифрование с открытым ключом. Алгоритм RSA.

4.9. Понятие и свойства хэш-функции. Электронная шифровая подпись.

4.10. Обзор современных отечественных и зарубежных стандартов шифрования и ЭЦП.

4.11. Понятие криптографического протокола.

4.12. Протоколы обмена ключами. Алгоритм Диффи-Хеллмана. Атака «человек посередине».

4.13. Алгоритмы генерации псевдослучайных последовательностей.

Раздел 5. Идентификация и аутентификация

5.1. Понятия идентификации и аутентификации. Виды аутентификации. Типология протоколов аутентификации.

5.2. Строгая односторонняя аутентификация на основе случайных чисел. Строгая двусторонняя аутентификация на основе случайных чисел. Аутентификация на основе асимметричного алгоритма.

5.3. Протокол Kerberos.

5.4. Механизмы аутентификации при осуществлении подключений. Протокол PPP CHAP. Протокол PPP EAP. Стандарт IEEE 802.1x

5.5. Аутентификация в защищенных соединениях. Протоколы SSL, TLS, SSH, S-HTTP, SOCKS. Семейство протоколов IPSec.

Раздел 6. Протоколирование и аудит

6.1. Понятие и назначение протоколирования и аудита. Подход к протоколированию в «Оранжевой книге».

6.2. Активный аудит. Сигнатура атаки. Функциональные компоненты и архитектура систем активного аудита.

Раздел 7. Компьютерные вирусы

7.1. Общие сведения о компьютерных вирусах. Структура вируса. Классификации вирусов.

7.2. Файловые вирусы и макровирусы. Загрузочные вирусы. Сетевые черви. Другие классы вредоносных программ: троянские кони, логические бомбы.

7.3. Технологии маскировки вирусов. Тенденции современных компьютерных вирусов.

7.4. Понятие антивируса. Методы обнаружения зараженных файлов. Обзор современных антивирусов.

7.5. Развертывание системы антивирусной защиты.

Раздел 8. Средства защиты сети

8.1. Межсетевые экраны.

8.2. Виртуальные частные сети.

8.3. Системы обнаружения вторжений. Анализ защищенности системы.

Раздел 9. Средства и методы противодействия угрозам доступности информации

9.1. Понятие и основные угрозы доступности информации. Показатели эффективности системы. Коэффициент готовности.

9.2. Методы обеспечения отказоустойчивости. Нейтрализация отказов. Живучесть. Резервирование. Программное обеспечение промежуточного слоя.

9.3. Архитектурные принципы обеспечения обслуживаемости. Восстановление после отказов.

Раздел 10. Основные принципы построения систем защиты

10.1. Меры противодействия угрозам безопасности.

10.2. Принципы построения систем защиты.

10.3. Понятие и назначение модели безопасности.

10.4. Модель дискреционного доступа. Модель Белла-ЛаПадулы. Ролевая модель контроля доступа.

10.5. Системы разграничения доступа

Раздел 11. Информационная безопасность с точки зрения технологии программирования

11.1. Основные принципы разработки безопасных систем.

11.2. Основные ошибки программирования. Причины и последствия переполнения буфера.

11.3. Анализ некоторых программных реализаций сервисов безопасности.

Раздел 12. Техника и методология атаки

12.1. Стратегия злоумышленника. Внешний анализ системы. Сканирование портов. Методы определения программно-аппаратной конфигурации системы и способы противодействия. Системы автоматического сканирования.

12.2. Использование уязвимостей в программном обеспечении. Эксплойты. Примеры наиболее известных уязвимостей в современных компьютерных системах.

12.3. Виды популярных атак и средства противодействивя. SQL-инъекции. Межсайтовый скриптинг.

5. Образовательные технологии, применяемые при освоении дисциплины

В рамках преподавания дисциплины используются следующие образовательные технологии: чтение лекций, проведение консультаций, практические занятия, ролевые игры, мастер-классы экспертов и специалистов.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются адаптивные образовательные технологии, подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, применение соответствующих методик по работе с инвалидами, использование средств дистанционного общения.

Для обеспечения дифференцированного подхода обеспечивается многоуровневая подача материала в соответствие с индивидуальными особенностями, предоставление учащимся права выбора целей, средств, форм работы, организация работы учащихся в малых группах, самостоятельная работа в собственном диапазоне возможностей, оценка достижения учащихся в соответствии с их возможностями.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе они должны составлять не менее 20% аудиторных занятий. Занятия лекционного типа для соответствующих групп студентов не могут составлять более 50% аудиторных занятий.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Контрольные работы

Контрольная работа № 1. Программная реализация шифратора / дешифратора для заданного алгоритма симметричного шифрования.

Задание: используя произвольный язык программирования (для выполнения задания в дисплейных классах рекомендуется язык Java), написать программу, осуществляющую шифрование и дешифрование произвольного текста в соответствии с заданным алгоритмом шифрования.

Минимальные возможности программы: загрузка и сохранение в файле шифруемого/дешифруемого текста и результата, загрузка и сохранение в файле ключа. Реализовать наглядное представление ключа в таких алгоримах как решетка Флейберга, шифр Плейфейера. Реализовать проверку допустимости ключа в таких алгоритмах как шифр Гронсфельда.

Варианты контрольной работы:

1) Шифр Гронсфельда
2) Шифр Бэкона
3) Перестановочный шифр
4) Шифр Тритемиуса
5) Шифр Плейфейера
6) Шифр простой замены
7) Квадратичная решетка
8) Шифр Хилла
9) Шифр Вернама
10) Скремблирующая последовательность на основе линейного генератора случайных чисел
11) Скремблирующая последовательность на основе квадратичного генератора случайных чисел.

Контрольная работа № 2. Программная реализация заданного криптографического протокола.

Задание: используя произвольный язык программирования (для выполнения задания в дисплейных классах рекомендуется язык Java), написать программу, реализующую заданный криптографический протокол.

Минимальные требования к программе: графический интерфейс пользователя, сетевое взаимодействие участников протокола, клиент для имитации атаки «человек посередине».

Варианты контрольной работы:

1) Строгая односторонняя аутентификация на основе случайных чисел;
2) Строгая двусторонняя аутентификация на основе случайных чисел;

3) Протокол Диффи-Хеллмана
4) Протокол одновременной подписи
5) Протокол групповой подписи
6) Протокол голосования
7) Протокол электронной цифровой подписи (использовать сторонние реализации функций хэширования и асимметричного шифрования).
8) Аутентификация на основе асимметричного алгоритма (использовать стороннюю реализации функций хэширования и асимметричного шифрования).

Контрольная работа № 3. Разработка политики безопасности и модели угроз для заданной организации.

Задание: студент получает адрес сайта некоторой организации. Используя открытые информационные источники, необходимо проанализировать деятельность этой организации и составить модель угроз для заданной организации, а затем, на основе модели угроз разработать политику безопасности.

Варианты контрольной работы (виды организаций, конкретные адреса сайтов могут меняться):

1) Университет;
2) Министерство субъекта федерации;
3) Интернет-магазин;
4) Библиотека;
5) Производственное предприятие;
6) Редакция;
7) Банк;
8) Страховая компания;
9) Ломбард;
10) Инвестиционный фонд;
11) Адвокатский кабинет;
12) Транспортная компания.

Контрольная работа № 4. Комплексный анализ защищенности информационной системы организации.

Студенты получают индивидуальные образы виртуальной машины с установленной и настроенной информационной системой некоторой организации. Задача: смонтировать виртуальный образ, запустить и проанализировать его. Выявить потенциальные уязвимости системы, устранить возможные проблемы безопасности, используя репозиторий свободного программного

обеспечения, разработать рекомендации по приобретению необходимого оборудования и ПО (а также их настройке) для ликвидации остальных угроз.

Примерные задания для проведения зачета (в форме тестирования)

1. Какие из этих утверждений, относящихся к шифру Плейфейра, верны?

а) в основе ключа шифра Плейфейера лежит кодовое слово (или фраза);

б) шифр Плейфейера относится к перестановочным шифрам;

в) единицей шифрования в шифре Плейфейера является биграмма;

г) шифр Плейфейера не скрывает полностью статистические особенности исходного текста.

2. Какие предположения включает неформальная модель нарушителя?

а) о мотивах нарушителя;

б) о категориях лиц, к которым может принадлежать нарушитель;

в) о социальном статусе нарушителя;

г) о предыдущих атаках, осуществленных нарушителем;

д) о времени действия нарушителя.

3. Какие объектамы наиболее подвержены угрозам ИБ в сфере экономики (согласно доктрине информационной безопасности РФ)?

а) система государственной статистики;

б) информационные ресурсы федеральных органов исполнительной власти и СМИ;

в) системы управления сложными исследовательскими комплексами (ядерными реакторами, ускорителями элементарных частиц, плазменными генераторами и другими);

г) системы бухгалтерского учета;

д) кредитно-финансовая система.

4. Подстановочный алгоритм шифрования — это...

а) способ шифрования, при котором каждый символ (или последовательность символов) исходного сообщения заменяются другим символом (или другой последовательностью символов);

б) способ шифрования, при котором один и тот же ключ используется и для шифрования и для расшифрования текста;

в) способ шифрования, при котором используются два свзяанных ключа: один для шифрования, другой для расшифрования;

г) способ шифрования, при котором символы открытого текста изменяют порядок следования в соответствии с правилом, которое определяется ключом.

5. В каком из представлений матрицы доступа наиболее просто определить файлы, доступ к которым имеет конкретный пользователь?

а) ACL;

б) списки полномочий субъектов;

в) атрибутные схемы.

6. Каков основной недостаток обнаружения вирусов методом эмуляции программ?

а) значительная вероятность ложного срабатывания;

б) крайне медленная работа антивируса;

в) невозможность обнаружения новых вирусов;

г) необходимость трудоемкой ручной настройки антивируса.

7. Расшифруйте текст «ПУЁПЭ» (использован шифр Гронсфельда с ключом 12).

8. Как называется свойство современных симметричных алгоритмов: отсутствие статистической взаимосвязи между ключом и зашифрованным текстом?

9. Зашифруйте сообщение 01011 скремблером 101 с ключом 101

10. Какой метод криптоанализа используется для взлома одного раунда шифрования блочного шифра на основе прослеживания изменений схожести между двумя текстами?

а) дифференциальный;

б) статистический;

в) линейный.

11. Открытым ключом RSA является пара (15, 2). Зашифруйте число 5.

12. Чтобы зашифровать сообщение с помощью асимметричного алгоритма шифрования используются:

а) открытый ключ отправителя;

б) открытый ключ получателя;

в) закрытый ключ отправителя;

г) закрытый ключ получателя.

13. Криптографическая стойкость алгоритма RSA основана на:

а) математическом аппарате эллиптических кривых;

б) произведении двух больших простых чисел;

в) сложности разложения на множители больших чисел;

г) сложности дискретного логарифмирования.

14. Какие свойства безопасности могут обеспечиваться посредством ЭЦП?

а) конфиденциальность;

б) целостность;

в) доступность;

г) апеллируемость;

д) аутентичность.

15. Протокол Диффи-Хеллмана — это:

а) протокол аутентификации;

б) протокол обмена ключами;

в) протокол одновременной подписи;

г) протокол групповой подписи;

д) протокол голосования.

16. Администратор закрыл для сотрудников организации доступ в Интернет, разрешив лишь пользование электронной почтой. К какому виду мер защиты информации относится данная мера?

а) политика безопасности верхнего уровня;

б) политика безопасности среднего уровня;

в) политика безопасности нижнего уровня;

г) принцип минимизации привилегий;

д) защита поддерживающей инфраструктуры.

17. Модель безопасности Белла-ЛаПадулы...

а) ... устанавливает различные уровни «секретности» объектов и субъектов доступа;

б) ... устанавливает набор разрешенных операций доступа для каждой пары «субъект-объект»;

в) ... привязывает набор разрешенных действий к роли, которую выполняет пользователь;

г) ... запрещает некоторым субъектам определенные виды доступа к некоторым объектам.

18. Какие утверждение о протоколе строгой односторонней аутентификации на основе случайных чисел справедливы?

а) в основе протокола лежит симметричный алгоритм шифрования;

б) на первом шаге проверяющий В отправляет проверяемому А случайное число;

в) на втором шаге проверяемый А отправляет проверяющему В зашифрованное сообщение, содержащее полученное на первом шаге случайное число, а также новое случайное число.

г) всего протокол требует отправки двух сообщений.

19. Какому требованию должен удовлетворять пароль для противодействия атаке методом социального инжиниринга?

а) пароль не должен быть производным от слов любого естественного языка;

б) длина пароля должна составлять 12 и более символов;

в) пароль нельзя открывать никому;

г) разные сервисы должны защищаться разными паролями;

д) пароль должен включать символы разных алфавитов и регистров, цифры, знаки препинания и т.д.

20. Какие недостатки имеют системы обнаружения вторжений, защищающие сегмент сети?

а) высокий процент ложных срабатываний;

б) не способны контролировать ситуацию во всей сети;

в) неспособны анализировать степень проникновения;

г) работа затруднена при высокой загрузке сети;

д) снижается эффективность работы сервера, на котором они установлены.

21. Какие вирусы заражают файлы, дописывая в них свою копию?

а) файловые вирусы;

б) загрузочные вирусы;

в) макровирусы;

г) сетевые черви;

д) троянские кони.

22. Каким образом проникают в систему сетевые черви?

а) по электронной почте;

б) любым способом вместе с зараженными ими файлами;

в) злоумышленник должен вручную внести вирус в систему;

г) через Интернет, используя ошибки в сетевых программах;

д) через съемные носители данных при срабатывании автозагрузки с них.

23 ... — комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.

24. Как называется свойство информации, позволяющее достоверно установить ее автора?

а) целостность;

б) апеллируемость;

в) доступность;

г) конфиденциальность;

д) аутентичность.

Примерные экзаменационные вопросы:

- Свойства компьютерной информации, важные с точки зрения информационной безопасности: конфиденциальность, целостность и доступность.
- Угрозы информационной безопасности.

- Каналы утечки информации.
- Неформальная модель нарушителя.
- Обзор стандартов и нормативно-правовой базы в сфере информационной безопасности.
- Сигналы, данные и методы получения информации. Свойства информации.
- Количество информации как мера уменьшения неопределенности знаний. Алфавитный подход к вычислению количества информации.
- Определение вероятности и основные правила вычисления количества информации.
- Информационная модель Шеннона.
- Формулы Шеннона и Хартли.
- Понятие кода. Связь между информационной емкостью и средней длиной кода. Избыточность кодирования.
- Метод сжатия по Хаффману.
- Код Хэмминга
- Множества и отношения. Бинарные отображения.
- Основная теорема арифметики. Алгоритм деления в Z.
- Понятие группы. Изоморфизмы групп.
- Понятие и свойства колец. Кольцо вычетов.
- Понятие поля. Поля Галуа.
- Кольца многочленов. Алгоритм деления в A[X]. Разложение в кольце многочленов. Неприводимые многочлены.
- Китайская теорема об остатках
- Эллиптические кривые.
- Понятие симметричных алгоритмов шифрования.
- Обзор классических симметричных алгоритмов. Моноафавитный шифр. Шифр Гронсфельда. Шифр Плейфейера. Шифр Хилла. Одноразовый блокнот. Перестановочные шифры.
- Диффузия и коффузия. Схема Файстеля.
- Обзор современных симметричных алгоритмов шифрования. Шифр DES. Шифр AES.
- Режимы функционирования блочных шифров.
- Скремблеры.
- Виды криптоанализа симметричных алгоритмов.
- Шифрование с открытым ключом. Алгоритм RSA.
- Понятие и свойства хэш-функции.

- Электронная шифровая подпись.
- Обзор современных отечественных и зарубежных стандартов шифрования и ЭЦП.
- Понятие криптографического протокола.
- Протоколы обмена ключами. Алгоритм Диффи-Хеллмана. Атака «человек посередине».
- Алгоритмы генерации псевдослучайных последовательностей.
- Понятия идентификации и аутентификации. Виды аутентификации. Типология протоколов аутентификации.
- Строгая односторонняя аутентификация на основе случайных чисел. Строгая двусторонняя аутентификация на основе случайных чисел. Аутентификация на основе асимметричного алгоритма.
- Протокол Kerberos.
- Механизмы аутентификации при осуществлении подключений. Протокол PPP CHAP. Протокол PPP EAP. Стандарт IEEE 802.1x
- Аутентификация в защищенных соединениях. Протоколы SSL, TLS, SSH, S-HTTP, SOCKS. Семейство протоколов IPSec.
- Понятие и назначение протоколирования и аудита. Подход к протоколированию в «Оранжевой книге».
- Активный аудит. Сигнатура атаки. Функциональные компоненты и архитектура систем активного аудита.
- Общие сведения о компьютерных вирусах. Структура вируса. Классификации вирусов.
- Файловые вирусы и макровирусы. Загрузочные вирусы. Сетевые черви. Другие классы вредоносных программ: троянские кони, логические бомбы.
- Технологии маскировки вирусов. Тенденции современных компьютерных вирусов.
- Понятие антивируса. Методы обнаружения зараженных файлов. Обзор современных антивирусов.
- Развертывание системы антивирусной защиты.
- Межсетевые экраны.
- Виртуальные частные сети.
- Системы обнаружения вторжений. Анализ защищенности системы.
- Понятие и основные угрозы доступности информации. Показатели эффективности системы. Коэффициент готовности.

- Методы обеспечения отказоустойчивости. Нейтрализация отказов. Живучесть. Резервирование. Программное обеспечение промежуточного слоя.
- Архитектурные принципы обеспечения обслуживаемости. Восстановление после отказов.
- Меры противодействия угрозам безопасности.
- Принципы построения систем защиты.
- Понятие и назначение модели безопасности.
- Модель дискреционного доступа. Модель Белла-ЛаПадулы. Ролевая модель контроля доступа.
- Системы разграничения доступа
- Основные принципы разработки безопасных систем.
- Основные ошибки программирования. Причины и последствия переполнения буфера.
- Анализ некоторых программных реализаций сервисов безопасности.
- Стратегия злоумышленника.
- Использование уязвимостей в программном обеспечении.
- SQL-инъекции.
- Межсайтовый скриптинг.

7. Данные для учета успеваемости студентов в БАРС

Таблица 1. Таблица максимальных баллов по видам учебной деятельности.

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
7	20	20	0	0	0	20	40	100
8	20	20	0	0	0	20	40	100

Программа оценивания учебной деятельности студента

7 семестр
Лекции
Оценивается посещаемость, активность, умение выделить главную мысль и др. Преподаватель выдает красивые именные карточки с изображением болот и равнин (а также островов) за попытки студентов сказать что-то умное и по-

участвовать в дискуссии. В конце семестра карточки подсчитываются и пропорционально начисляются баллы. Максимальный балл (20) получает обладатель наибольшего числа карточек.

Лабораторные работы
Оценивается самостоятельность при выполнении работы, грамотность в оформлении, правильность выполнения и т.д. Заработать можно максимум 20 баллов, которые начисляются преподавателем за решение поставленных задач (программирование, работа в программах и т.д.)

Другие виды учебной деятельности
Контрольная работа №1- от 0 до 20 баллов
Критерии оценки:
Оценивается правильность и полнота выполнения задания, обоснованность основных выводов, корректность изложение результата.

Промежуточная аттестация
Проходит в виде устного ответа по билетам. Максимально возможный балл 40.
При проведении промежуточной аттестации
ответ на «отлично» оценивается от 30 до 40 баллов;
ответ на «хорошо» оценивается от 20 до 30 баллов;
ответ на «удовлетворительно» оценивается от 10 до 20 баллов;
ответ на «неудовлетворительно» оценивается от 0 до 10 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за 7 семестр по дисциплине «Математические основы информационной безопасности» составляет 100 баллов.

Таблица 2.1 Таблица пересчета полученной студентом суммы баллов по дисциплине «Математические основы информационной безопасности» за 7 семестр в оценку (зачет):

50 баллов и более	«зачтено»
меньше 50 баллов	«не зачтено»

8 семестр
Лекции
Оценивается посещаемость, активность, умение выделить главную мысль и др. Преподаватель выдает красивые именные карточки с изображением болот и равнин (а также островов) за попытки студентов сказать что-то умное и поучаствовать в дискуссии. В конце семестра карточки подсчитываются и про-

порционально начисляются баллы. Максимальный балл (20) получает обладатель наибольшего числа карточек.

Лабораторные работы
Оценивается самостоятельность при выполнении работы, грамотность в оформлении, правильность выполнения и т.д. Заработать можно максимум 20 баллов, которые начисляются преподавателем за решение поставленных задач (программирование, работа в программах и т.д.)

Другие виды учебной деятельности
Контрольная работа №2- от 0 до 20 баллов
Критерии оценки:
Оценивается правильность и полнота выполнения задания, обоснованность основных выводов, корректность изложение результата.
Промежуточная аттестация
Проходит в виде устного ответа по билетам. Максимально возможный балл 40.
При проведении промежуточной аттестации
ответ на «отлично» оценивается от 30 до 40 баллов;
ответ на «хорошо» оценивается от 20 до 30 баллов;
ответ на «удовлетворительно» оценивается от 10 до 20 баллов;
ответ на «неудовлетворительно» оценивается от 0 до 10 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за 8 семестр по дисциплине «Математические основы информационной безопасности» составляет 100 баллов.

Таблица 2.2 Таблица пересчета полученной студентом суммы баллов по дисциплине «Математические основы информационной безопасности» за 8 семестр в оценку (экзамен):

100-80 баллов	«отлично»
80-60 баллов	«хорошо»
60-40 баллов	«удовлетворительно»
40-0 баллов	«не удовлетворительно»

8. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

- Ярочкин В.И. Информационная безопасность [Текст] : учеб. для студентов вузов, обучающихся по гуманитар. и социал.-экон. специальностям / В. И. Ярочкин. - М. : Гаудеамус : Акад. Проект, 2008.
- Информационная безопасность и защита информации [Текст] : учеб. пособие для студентов вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - 4-е изд., стер. - М. : Изд. центр "Академия", 2009.
- Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Башлы П. Н. – Москва: Евразийский открытый институт, 2012. -311 c. 978-5-374-00301-7

Книга находится в базовой версии ЭВС IPRbooks/

б) дополнительная литература:

- А. А. Малюк. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст] : учеб. пособие / А. А. Малюк. - М. : Горячая линия - Телеком, 2004.
- И.Р. Конеев. Информационная безопасность предприятия [Текст] : [учеб. пособие] / И. Р. Конеев, А. В. Беляев. - СПб. : БХВ-Петербург, 2003.
- Информационная безопасность систем организационного управления. Теоретические основы [Текст] : в 2 т. / Н. А. Кузнецов [и др.] ; под ред. Н. А. Кузнецова, В. В. Кульбы ; Рос. акад. наук, Ин-т проблем передачи информ. - М. : Наука, 2006.
- Криптография на Си и C++ в действии [Текст] : учеб. пособие / М. Вельшенбах. - М. : Триумф, 2004.
- Смарт Н. Криптография [Текст] / Н. Смарт ; пер. с англ. С. А. Кулешова ; под ред. С. К. Ландо. - М. : Техносфера, 2006.
- О. А. Логачев, А. А. Сальников, В. В. Ященко. Булевы функции в теории кодирования и криптологии. – М.: МЦНМО, 2004 г.
- • Брюс Шнайер. Секреты и ложь. Безопасность данных в цифровом мире. СПб.: Питер, 2003.

в) Рекомендуемая литература

- А. Ю. Зубов. Математика кодов аутентификации. – М.: Гелиос АРВ, 2007.
- Фомичев В.М. Методы дискретной математики в криптологии. – М.: Диалог-МИФИ, 2010.
- Касперски К. Записки исследователя компьютерных вирусов. – СПб.: Питер, 2005.
- Ховард М., Лебланк Д., Вьега Дж. 24 смертных греха компьютерной безопасности. Библиотека программиста. – СПб., Питер, 2010.
- Шаныгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. — М.: ИД «ФОРУМ»: ИНФРА-М, 2008.
- Элсенпитер Р., Тоби Дж. Велт. Администрирование сетей Microsoft Windows XP Professional. Эком, 2006.
- Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография — М.: Норма, 2004

г) Интернет-ресурсы

- Портал по информационной безопасности http://www.securitylab.ru/
- Учебные ресурсы центра «Новые информационные технологии» http://nto.immpu.sgu.ru

9. Материально-техническое обеспечение дисциплины

Материально-техническое обеспечение дисциплины «Математические основы информационной безопасности» составляют: мультимедийная лекционная аудитория с проектором и интерактивной доской, компьютерный класс. Необходим доступ в Интернет и любая среда программирования (рекомендуется Java на платформе разработки Eclipse).

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 38.03.05 «Бизнес-информатика».

Автор – *Р. В. Амелин*.

Программа разработана 2016 году (одобрена на заседании кафедры математической теории упругости и биомеханики от 31.08.2016 года, протокол №1).

Зав. кафедрой
математической теории упругости и биомеханики
д.ф.-м.н., профессор Л.Ю. Коссович

Декан механико-математического факультета
к.ф.-м.н., доцент А.М. Захаров

9. Материально-техническое обеспечение дисциплины

Материально-техническое обеспечение дисциплины «Математические основы информационной безопасности» составляют: мультимедийная лекционная аудитория с проектором и интерактивной доской, компьютерный класс. Необходим доступ в Интернет и любая среда программирования (рекомендуется Java на платформе разработки Eclipse).

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 38.03.05 «Бизнес-информатика».

Автор – *Р. В. Амелин*.

Программа разработана 2016 году (одобрена на заседании кафедры математической теории упругости и биомеханики от 31.08.2016 года, протокол №1).

Зав. кафедрой
математической теории упругости и биомеханики
д.ф.-м.н., профессор Л.Ю. Коссович

Декан механико-математического факультета
к.ф.-м.н., доцент А.М. Захаров