МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Минзарипов Р.Г.

подписано электронно-цифровой подписью

Программа дисциплины

Информационная безопасность и защита информации Б3.В.5

Направление подготовки: 010400.62 - Прикладная математика и информатика
Профиль подготовки: Математическая кибернетика
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Автор(ы):
Гайнутдинова А.Ф.
Рецензент(ы):
Гусенков А.М.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Аблаев Ф. М.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 927515

Казань
2015

Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Программу дисциплины разработал(а)(и) доцент, к.н. Гайнутдинова А.Ф. кафедра теоретической кибернетики отделение фундаментальной информатики и информационных технологий , Aida.Gainutdinova@kpfu.ru

1. Цели освоения дисциплины

В курсе рассматриваются основные положения информационной безопасности и защиты информации.Рассматриваются основные законодательные акты, касающиеся вопросов информационной безопасности. Вводится понятие информации с точки зрения предмета защиты информации, определяются основные категории, которым должна удовлетворять информация. Вводятся понятие атака на информацию, рассматриваются основные виды атак, последствия от них. Вводится понятие информационная система, информационная сеть, рассматриваются основные виды угроз на них и способы защиты от этих угроз. Для распределенных компьютерных сетей возможные виды угроз передачи информации рассматриваются с привязкой их к уровням модели межсетевого взаимодействия OSI.Рассматриваются основные стандарты и спецификации в области информационной безопасности, как международные, так и российские, изучаются основные понятия, определенные в них.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б3.В.5 Профессиональный" основной образовательной программы 010400.62 Прикладная математика и информатика и относится к вариативной части. Осваивается на 4 курсе, 7 семестр.

Данная дисциплина относится к профессиональным дисциплинам.

Читается на 4 курсе 7 семестр для студентов, обучающихся по направлению "Прикладная математика и информатика".

Для освоения данного курс студент должен прослушать курсы "Введение в криптографию", "Современные информационные технологии", "Архитектура компьютеров".

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-16 (общекультурные компетенции)	способностью к интеллектуальному, культурному, нравственному, физическому и профессиональному саморазвитию, стремление к повышению своей квалификации и мастерства
ПК-12 (профессиональные компетенции)	способностью составлять и контролировать план выполняемой работы, планировать необходимые для выполнения работы ресурсы, оценивать результаты собственной работы
ПК-8 (профессиональные компетенции)	способностью формировать суждения о значении и последствиях своей профессиональной деятельности с учетом социальных, профессиональных и этических позиций
ПК-7 (профессиональные компетенции)	способностью собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным, профессиональным, социальным и этическим проблемам

В результате освоения дисциплины студент:

1. должен знать:

законодательный морально-этический, административно-процедурный, физический, аппаратно-программный аспекты обеспечения информационной безопасности; существующие способы защиты информации этапах хранения, обработки, передачи информации в целях сохранения ее необходимых качеств, таких, как доступность, целостность, конфиденциальность, аппелируемость, аутентичность;

2. должен уметь:

ориентироваться в методах защиты информации и в том, когда и каким они применяются.

3. должен владеть:

теоретическими знаниями о существующих способах защиты информации на всех этапах: хранения, обработки, передачи информации в целях сохранения необходимых качеств, таких, как доступность, целостность, конфиденциальность, аппелируемость, аутентичность, навыками организации защиты информационных систем.;

4. должен демонстрировать способность и готовность:

готовность и способность применять полученные знания на практике.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) 108 часа(ов).

Форма промежуточного контроля дисциплины зачет в 7 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Информация как объект защиты. Законодательные основы по защите информации.	7	1	0	0	2	устный опрос

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
2.	Тема 2. Понятие информации. Основные качества информации с точки зрения информационной безопасности. Понятие информационной системы.	7	2	0	0	2	устный опрос
3.	Тема 3. Угрозы информационной системы (случайные, преднамеренные воздействия).	7	3	0	0	2	устный опрос
4.	Тема 4. Информационные компьютерные сети. Удаленные атаки. Особенности защиты информации в компьютерных сетях.	7	3	0	0	4	устный опрос
5.	Тема 5. Стандарты и спецификации в области информационной безопасности.	7	4	0	0	2	устный опрос
6.	Тема 6. Избирательная и полномочная политика безопасности.	7	5	0	0	2	устный опрос
7.	Тема 7. Административный уровень обеспечения информационной безопасности.	7	6	0	0	2	устный опрос
8.	Тема 8. Процедурный уровень обеспечения информационной безопасности.	7	7	0	0	2	устный опрос
9.	Тема 9. Обзор аппаратно-программных средств защиты информации.	7	8	0	0	2	устный опрос
10.	Тема 10. Обзор модели межсетевого взаимодействия OSI. Уровни сетевых атак согласно модели OSI.	7	9	0	0	2	устный опрос

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
11.	Тема 11. Предмет и задачи криптографии и криптоанализа.	7	10	0	0	2	письменная работа
12.	Тема 12. Симметричные системы шифрования.	7	11	0	0	4	устный опрос
13.	Тема 13. Ассиметричные системы шифрования.	7	12	0	0	4	устный опрос
14.	Тема 14. Теория сложности и криптография. Односторонние функции, Хеш-функции. Их свойства и использование в криптографии.	7	13	0	0	4	устный опрос
15.	Тема 15. Ассиметричные криптоалгоритмы. Алгоритм RSA.	7	14	0	0	4	устный опрос
16.	Тема 16. Электронно-цифровая подпись.	7	15	0	0	2	устный опрос
17.	Тема 17. Средства управления криптографическими ключами.	7	16	0	0	4	устный опрос
18.	Тема 18. Криптографические протоколы	7	17	0	0	4	устный опрос
19.	Тема 19. Квантовая криптография.	7	18	0	0	4	письменная работа
.	Тема . Итоговая форма контроля	7		0	0	0	зачет
	Итого			0	0	54	

4.2 Содержание дисциплины

Тема 1. Информация как объект защиты. Законодательные основы по защите информации.

лабораторная работа (2 часа(ов)):

Информация как объект защиты. Законодательные основы по защите информации (Федеральный закон "Об информации, информатизации и защите информации", Закон "О коммерческой тайне", Закон "О банках и банковской деятельности в РФ"и др.). Цели защиты информации. Атака на информацию. Экономические и моральные последствия атаки на информацию. Пять уровней обеспечения информационной безопасности (системы защиты): Законодательный, Морально-этический, Административный, Физический, Аппаратно-программный. Основные принципы выстраивания надежной системы защиты.

Тема 2. Понятие информации. Основные качества информации с точки зрения информационной безопасности. Понятие информационной системы.

лабораторная работа (2 часа(ов)):

Понятие информации. Основные качества информации с точки зрения информационной безопасности: доступность, конфиденциальность, целостность, аутентичность, апеллируемость.

Тема 3. Угрозы информационной системы (случайные, преднамеренные воздействия).

лабораторная работа (2 часа(ов)):

Понятие информационной системы. Классификация информационных систем по сфере применения и по масштабности. Основные качества информационных систем с точки зрения информационной безопасности (надежность, точность контроль доступа, контролируемость, контроль идентификации, устойчивость к умышленным сбоям). Основные компоненты информационной системы (аппаратные средства, программное обеспечение, данные, персонал). Их роль в обеспечении информационной безопасности. Угрозы информационной системы (случайные, преднамеренные воздействия). Примеры случайных воздействий на информационную систему. Преднамеренные воздействия. Несанкционированный доступ как наиболее распространенный вид преднамеренного воздействия. Основные каналы несанкционированного доступа к информационной системе. Обзор наиболее распространенных методов взлома.

Тема 4. Информационные компьютерные сети. Удаленные атаки. Особенности защиты информации в компьютерных сетях.

лабораторная работа (4 часа(ов)):

Информационные компьютерные сети. Удаленные атаки. Особенности защиты информации в компьютерных сетях. Атакуемые сетевые компоненты. Основные компоненты (сервера, рабочие станции, среда передачи информации, узлы коммутации сетей), их функции. Виды атак на сетевые компоненты. Атаки на DNS- сервера. Логические доменные адреса и их IP-адреса. Атаки на рабочие станции. ?Троянские программы? как разновидность компьютерных вирусов. Способы борьбы с троянскими программами.

Тема 5. Стандарты и спецификации в области информационной безопасности.

лабораторная работа (2 часа(ов)):

Стандарты и спецификации в области информационной безопасности: стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем" (Оранжевая книга), "Гармонизированные критерии Европейских стран", международный стандарт "Критерии оценки безопасности информационных технологий", Руководящие документы Гостехкомиссии России. Обзор понятийного аппарата, определенного в этих документах.

Тема 6. Избирательная и полномочная политика безопасности.

лабораторная работа (2 часа(ов)):

Основные понятия: избирательная и полномочная политика безопасности, управление информационными потоками, доверенная вычислительная база, монитор обращений, доверенный вычислительный путь, периметр безопасности.

Тема 7. Административный уровень обеспечения информационной безопасности.

лабораторная работа (2 часа(ов)):

Процедурный уровень обеспечения информационной безопасности: управление персоналом; физическая защита; поддержание работоспособности; реагирование на нарушения режима безопасности; планирование восстановительных работ.

Тема 8. Процедурный уровень обеспечения информационной безопасности.

лабораторная работа (2 часа(ов)):

Системы шифрования дисковых данных. Системы шифрования данных, передаваемых по сетям. Два способа: канальное шифрование и оконечное (абонентское шифрование). Преимущества и недостатки.

Тема 9. Обзор аппаратно-программных средств защиты информации.

лабораторная работа (2 часа(ов)):

Обзор модели межсетевого взаимодействия OSI. Уровни сетевых атак согласно модели OSI.

Тема 10. Обзор модели межсетевого взаимодействия OSI. Уровни сетевых атак согласно модели OSI.

лабораторная работа (2 часа(ов)):

Предмет и задачи криптографии и криптоанализа. История развития криптографии. Стойкость криптографического алгоритма. Методы доказательства стойкости шифра. Классификация криптографических алгоритмов: В зависимости от наличия ключа: тайнопись (ограниченные алгоритмы) и критография. В зависимости от соответствия ключей шифрования и дешифрования: симметричные и асимметричные. В зависимости от типа используемых преобразований: перестановочные и подстановочные. В зависимости от размера шифруемого блока: потоковые и блочные шифры.

Тема 11. Предмет и задачи криптографии и криптоанализа.

лабораторная работа (2 часа(ов)):

Симметричные системы шифрования, их особенности, преимущества и недостатки. Предмет и задачи криптографии и криптоанализа. История развития криптографии. Стойкость криптографического алгоритма. Методы доказательства стойкости шифра. Классификация криптографических алгоритмов: В зависимости от наличия ключа: тайнопись (ограниченные алгоритмы) и критография. В зависимости от соответствия ключей шифрования и дешифрования: симметричные и асимметричные. В зависимости от типа используемых преобразований: перестановочные и подстановочные. В зависимости от размера шифруемого блока: потоковые и блочные шифры.

Тема 12. Симметричные системы шифрования.

лабораторная работа (4 часа(ов)):

Симметричные системы шифрования, их особенности, преимущества и недостатки. Генерация и распределение ключей шифрования. Виды подстановочных шифров. Виды перестановочных шифров. Механические шифровальные устройства, Роторные машины. Абсолютно стойкие шифры. Одноразовый блокнот.

Тема 13. Ассиметричные системы шифрования.

лабораторная работа (4 часа(ов)):

Ассиметричные системы шифрования, их особенности, преимущества и недостатки. Сравнение с симметричными системами. Генерация и распределение ключей шифрования для ассиметричных систем.

Тема 14. Теория сложности и криптография. Односторонние функции, Хеш-функции. Их свойства и использование в криптографии.

лабораторная работа (4 часа(ов)):

Теория сложности и криптография. Понятие односторонней функции. Использование односторонних функций в криптографических алгоритмах. Хеш-функции. Их свойства и использование в криптографии.

Тема 15. Ассиметричные криптоалгоритмы. Алгоритм RSA.

лабораторная работа (4 часа(ов)):

Ассиметричные криптоалгоритмы. Алгоритм RSA. Его краткая характеристика и применение в криптографии.

Тема 16. Электронно-цифровая подпись.

лабораторная работа (2 часа(ов)):

Электронно-цифровая подпись. Формирование ЭЦП и использование для защиты электронных документов от подделки. Удостоверяющие центры. Их основные задачи. Система удостоверяющих центров в России и за рубежом.

Тема 17. Средства управления криптографическими ключами.

лабораторная работа (4 часа(ов)):

Механизм распространения ключей. Обмен ключами по алгоритму Диффи-Хеллмана.

Тема 18. Криптографические протоколы

лабораторная работа (4 часа(ов)):

Обзор криптографических протоколов. Сферы применения данных протоколов.

Тема 19. Квантовая криптография.

лабораторная работа (4 часа(ов)):

Основы квантовой информатики. Алгоритмы квантового распределения ключа.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Информация как объект защиты. Законодательные основы по защите информации.	7	1	подготовка к устному опросу	2	устный опрос
2.	Тема 2. Понятие информации. Основные качества информации с точки зрения информационной безопасности. Понятие информационной системы.	7	2	подготовка к устному опросу	2	устный опрос
3.	Тема 3. Угрозы информационной системы (случайные, преднамеренные воздействия).	7	3	подготовка к устному опросу	2	устный опрос
4.	Тема 4. Информационные компьютерные сети. Удаленные атаки. Особенности защиты информации в компьютерных сетях.	7	3	подготовка к устному опросу	4	устный опрос
5.	Тема 5. Стандарты и спецификации в области информационной безопасности.	7	4	подготовка к устному опросу	2	устный опрос

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
6.	Тема 6. Избирательная и полномочная политика безопасности.	7	5	подготовка к устному опросу	2	устный опрос
7.	Тема 7. Административный уровень обеспечения информационной безопасности.	7	6	подготовка к устному опросу	2	устный опрос
8.	Тема 8. Процедурный уровень обеспечения информационной безопасности.	7	7	подготовка к устному опросу	2	устный опрос
9.	Тема 9. Обзор аппаратно-программных средств защиты информации.	7	8	подготовка к устному опросу	2	устный опрос
10.	Тема 10. Обзор модели межсетевого взаимодействия OSI. Уровни сетевых атак согласно модели OSI.	7	9	подготовка к устному опросу	2	устный опрос
11.	Тема 11. Предмет и задачи криптографии и криптоанализа.	7	10	подготовка к письменной работе	2	письменная работа
12.	Тема 12. Симметричные системы шифрования.	7	11	подготовка к устному опросу	4	устный опрос
13.	Тема 13. Ассиметричные системы шифрования.	7	12	подготовка к устному опросу	4	устный опрос
14.	Тема 14. Теория сложности и криптография. Односторонние функции, Хеш-функции. Их свойства и использование в криптографии.	7	13	подготовка к устному опросу	4	устный опрос
15.	Тема 15. Ассиметричные криптоалгоритмы. Алгоритм RSA.	7	14	подготовка к устному опросу	4	устный опрос
16.	Тема 16. Электронно-цифровая подпись.	7	15	подготовка к устному опросу	2	устный опрос
17.	Тема 17. Средства управления криптографическими ключами.	7	16	подготовка к устному опросу	4	устный опрос

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
18.	Тема 18. Криптографические протоколы	7	17	подготовка к устному опросу	4	устный опрос
19.	Тема 19. Квантовая криптография.	7	18	подготовка к письменной работе	4	письменная работа
	Итого				54	

5. Образовательные технологии, включая интерактивные формы обучения

происходит в форме лекций, лабораторных занятий. Рекомендуется поощрять активность студентов на занятии, отмечая в журнале и оценивая их активность в баллах. Проводить групповые и индивидуальные консультации студентов по вопросам, возникающим у студентов в ходе их подготовки к аттестации по учебной дисциплине, рекомендовать в помощь учебные и другие материалы, а также справочную литературу.

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

Тема 1. Информация как объект защиты. Законодательные основы по защите информации.

устный опрос , примерные вопросы:

Законодательные аспекты информационной безопасности.

Тема 2. Понятие информации. Основные качества информации с точки зрения информационной безопасности. Понятие информационной системы.

устный опрос , примерные вопросы:

Основные качества информации с точки зрения информационной безопасности. Охарактеризовать каждый аспект. Привести примеры нарушения этих качеств.

Тема 3. Угрозы информационной системы (случайные, преднамеренные воздействия).

устный опрос , примерные вопросы:

Характеризация угроз, примеры по каждому виду угроз.

Тема 4. Информационные компьютерные сети. Удаленные атаки. Особенности защиты информации в компьютерных сетях.

устный опрос , примерные вопросы:

Особенности угроз для распределенных информационных систем, примеры по каждому виду угроз.

Тема 5. Стандарты и спецификации в области информационной безопасности.

устный опрос , примерные вопросы:

Какие существуют стандарты в области информационной безопасности.

Тема 6. Избирательная и полномочная политика безопасности.

устный опрос , примерные вопросы:

Основные положения избирательной политики безопасности. Как она может реализоваться.

Тема 7. Административный уровень обеспечения информационной безопасности.

устный опрос , примерные вопросы:

Основные вопросы, которые выводятся на административный уровень обеспечения ИБ.

Тема 8. Процедурный уровень обеспечения информационной безопасности.

устный опрос , примерные вопросы:

Основные вопросы, которые выводятся на процедурный уровень обеспечения ИБ.

Тема 9. Обзор аппаратно-программных средств защиты информации.

устный опрос , примерные вопросы:

Основные группы аппаратно-программных средств ЗИ.

Тема 10. Обзор модели межсетевого взаимодействия OSI. Уровни сетевых атак согласно модели OSI.

устный опрос , примерные вопросы:

Характеристика модели OSI в том числе с точки зрения защиты информации.

Тема 11. Предмет и задачи криптографии и криптоанализа.

письменная работа , примерные вопросы:

Примерные варианты вопросов. 1. Какие Вы знаете государственные законы, касающиеся вопросов защиты информации и информационной безопасности. 2. Приведите примеры типов информации, которая является к категории конфиденциальной по определению. 3. Кто обеспечивает меры по обеспечению конфиденциальности информации. 4. Назовите 5 аспектов, которым должна удовлетворять информация с точки зрения защиты информации. 5. В чем их различие понятий аппелируемость и аутентичность. 6. Каковы требования должны выполняться для терминалов с физическим доступом с точки зрения информационной безопасности. 7. На какие компоненты можно разбить распределенную информационную систему. 8. Формирование режима информационной безопасности проблема комплексная. Меры по ее решению можно разделить на уровни. Назовите их. 9. На каком этапе должны начинаться действия по обеспечению информационной безопасности, касающиеся процедурного уровня, а именно управления персоналом. 10. Перечислите аппаратно-программные средства защиты информации. и .т.д.

Тема 12. Симметричные системы шифрования.

устный опрос , примерные вопросы:

Что такое симметричные системы шифрования. Примеры. Стойкость.

Тема 13. Ассиметричные системы шифрования.

устный опрос , примерные вопросы:

Что такое ассимметричные системы шифрования. Примеры. Стойкость.

Тема 14. Теория сложности и криптография. Односторонние функции, Хеш-функции. Их свойства и использование в криптографии.

устный опрос , примерные вопросы:

Математический аппарат криптографии.

Тема 15. Ассиметричные криптоалгоритмы. Алгоритм RSA.

устный опрос , примерные вопросы:

Подробный анализ системы RSA.

Тема 16. Электронно-цифровая подпись.

устный опрос , примерные вопросы:

Реализация ЭЦП. Сравнение с алгоритмами ассиметричного шифрования.

Тема 17. Средства управления криптографическими ключами.

устный опрос , примерные вопросы:

Основные задачи, связанные с управлением криптографическими ключами. Как они решаются.

Тема 18. Криптографические протоколы

устный опрос , примерные вопросы:

Обзор криптографических протоколов.

Тема 19. Квантовая криптография.

письменная работа , примерные вопросы:

Примерные варианты вопросов: 1. Какие факторы влияют на выбор метода шифрования информации с целью ее защиты. 2. Что такое стойкость шифра. 3. Сформулируйте принцип защиты информации о соотношении цены информации, цены затрат на ее защиту и затрат на ее добывание. 4. Назовите известные вам шифры, существовавшие в древности. 5. Какие существуют математические методы доказательства стойкости шифра. 6. Какие криптографические алгоритмы требуют согласования ключа. 7. Что такое ограниченный алгоритм шифрования. и т.д.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

По данной дисциплине предусмотрено проведение зачета. Примерные вопросы для зачета - Приложение 1.

Примерные вопросы к зачету:

1. Информация как объект защиты. Законодательные основы по защите информации. Цели защиты информации. Основные виды и источники атак на информацию.

2. Понятие информации. Основные категории информации с точки зрения информационной безопасности. Атака на информацию. Экономические и моральные последствия атаки на информацию.

3. Международные и российские стандарты и спецификации в области информационной безопасности. Обзор основных понятий и положений, изложенных в них.

и т.д.

7.1. Основная литература:

Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие, 2012. - URL: http://kpfu.ru/docs/F366166681/mzi.pdf

Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. URL: http://www.znanium.com/bookread.php?book=420047

Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. URL: http://www.znanium.com/bookread.php?book=405000

Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с. URL: http://znanium.com/bookread.php?book=335362

7.2. Дополнительная литература:

В. П. Мельников, С. А. Клейменов, А. М. Петраков. Информационная безопасность и защита информации: учеб. пособие для студ.высш.учеб.заведений / - М.: Академия, 2006. - 336 с.

Расторгуев С. П. Основы информационной безопасности: Учебное пособие. - М.: Академия, 2007. - 186 с.

7.3. Интернет-ресурсы:

Интернет-портал образовательных ресурсов КФУ - http://www.kfu-elearning.ru/

Интернет-портал образовательных ресурсов по ИТ - http://algolist.manual.ru/

Интернет-портал по математическим наукам - http://www.mathnet.ru

Интернет-портал ресурсов по математике - http://www.allmath.com/

Интернет-портал ресурсов по математическим наукам - http://www.math.ru/

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Информационная безопасность и защита информации" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен студентам. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Лекционные занятия по дисциплине проводятся в аудитории, оснащенной доской и мелом(маркером), а так же в специализированных компьютерных кабинетах.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010400.62 "Прикладная математика и информатика" и профилю подготовки Математическая кибернетика .

Автор(ы):
Гайнутдинова А.Ф. _____
"__" _____ 201 __ г.

Рецензент(ы):
Гусенков А.М. _____
"__" _____ 201 __ г.