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.
_____
"___"_____20___ г.

Программа дисциплины

Информационная безопасность Б3.Б.2.5

Направление подготовки: 230700.62 - Прикладная информатика
Профиль подготовки: Прикладная информатика в экономике
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Автор(ы):
Гайнутдинова Т.Ю.
Рецензент(ы):
Хакимов Р.Г.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Хакимов Р. Г.
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

Казань
2014

Содержание

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Гайнутдинова Т.Ю. кафедра информатики и вычислительных технологий отделение информационных технологий в гуманитарной сфере , Tatyana.Gajnutdinova@kpfu.ru

1. Цели освоения дисциплины

Цель курса - формирование систематизированных знаний в области построения Системы обеспечения информационной безопасности (СОИБ) объекта, защиты информации и информационной среды по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

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

Данная учебная дисциплина включена в раздел " Б3.Б.2 Профессиональный" основной образовательной программы 230700.62 Прикладная информатика и относится к базовой (общепрофессиональной) части. Осваивается на 4 курсе, 7 семестр.

Данная дисциплина "Информационная безопасность" входит в состав общепрофессиональных дисциплин Б 3.1.2.5, читается на 1 курсе во 2 семестре и на 2-м курсе 3. Знания, полученные при изучении этой дисциплине, потребуются далее при изучении таких дисциплин как "Проектирование информационных систем", "Сетевые операционные системы" и др., а также при написании выпускных квалификационных работ.

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-1 (общекультурные компетенции)	Владение культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
ОК-12 (общекультурные компетенции)	Способен понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности.
ОК-4 (общекультурные компетенции)	Способен использовать знания о современной естественнонаучной картине мира в образовательной и профессиональной деятельности, применять методы математической обработки информации, теоретического и экспериментального исследования.
ОК-9 (общекультурные компетенции)	Способен работать с информацией в глобальных компьютерных сетях.
ПК-2 (профессиональные компетенции)	Способность решать задачи воспитания и духовно-нравственного развития личности обучающихся.

В результате освоения дисциплины студент:

1. должен знать:

Должен знать:

- свойства информации, определяющие выбор средств и методов информационной защиты и влияющие на ее результативность,
- основное содержание, средства и методы используемых на практике или используемых на практике или развиваемых направлений информационной защиты,
- основные принципы, стратегии и модели информационной защиты,основные принципы, стратегии и модели информационной защционной защиты,- олоддо
- наиболее распространенные цели, способы и мотивы совершения преступлений с использованием компьютерных технологий, и типичные качества

личности преступников,

- составы преступлений в сфере компьютерной информации и толкование специальных терминов, употребляемых в них,
- принципы комплексирования средств и методов защиты информации.

2. должен уметь:

В результате изучения дисциплины студенты должны иметь представление:

- о комплексной системе защиты объектов информатизации;
- о разрабатываемых моделях информационной защиты;
- о государственной политике в информационной сфере;
- о правовых режимах защиты государственной тайны и конфиденциальной информации.

3. должен владеть:

Владеть:

- организационно-техническими и режимными мерами и методами;
- технологией защиты информации конкретной информационной системы;
- программно-техническими способами и средствами обеспечения информационной безопасности.

Применять программно-технические способы и средства для обеспечения информационной безопасности объекта.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы) 144 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. Свойства информации как объекта защиты	7	2	2	0	2	
2.	Тема 2. Методы контроля доступа к информации и ее инженерно-техническая защита	7	2	4	0	4	
3.	Тема 3. Информационные и компьютерные преступления как объекта защиты	7	2	4	0	2	
4.	Тема 4. Виды кодирования и их использование в защите информации	7	2	4	0	2	
5.	Тема 5. Обеспечение конфиденциальности и целостности информационных ресурсов	7	1	2	0	2	
6.	Тема 6. Лабораторная работа №1 Разграничение прав пользователей в защищенных версиях операционной системы Windows	7	2	2	0	2	
7.	Тема 7. Лабораторная работа №2 Реализация политики безопасности в защищенных версиях операционной системы Windows	7	2	4	0	4	
8.	Тема 8. Лабораторная работа №3 Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows	7	2	2	0	2	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
9.	Тема 9. Лабораторная работа ?4 Освоение средств защищенных версий операционной системы Windows, предназначенных для ? разграничения доступа субъектов к принтерам; ? разграничения доступа к разделам реестра; ? обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы.	7	2	2	0	4	
10.	Тема 10. Лабораторная работа ? 5 Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов	7	2	2	0	2	
11.	Тема 11. Лабораторная работа ?6 Определение правил для выбора защищенного пароля, определение слабо защищенного пароля, методы подбора пароля	7	2	2	0	2	
12.	Тема 12. Лабораторная работа ?7 Способы шифрования (дешифрования) или хеширования паролей	7	2	2	0	4	
13.	Тема 13. Лабораторная работа ?8 Создание комплексной защиты информации	7	2	2	0	2	
14.	Тема 14. Лабораторная работа ?9 Система фильтрации IP-трафика	7	2	2	0	2	

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
.	Тема . Итоговая форма контроля	7		0	0	0	зачет
	Итого			36	0	36	

4.2 Содержание дисциплины

Тема 1. Свойства информации как объекта защиты

лекционное занятие (2 часа(ов)):

1.1.Введение в информационную безопасность. 1.2. Уровни представления информации и особенности ее защиты. 1.3. Виды и общая характеристика информационных угроз. 1.4. Реализация информационной защиты.

лабораторная работа (2 часа(ов)):

Отчет по лабораторной работе.

Тема 2. Методы контроля доступа к информации и ее инженерно-техническая защита

лекционное занятие (4 часа(ов)):

2.1. Методы идентификации и аутентификации пользователей, технических средств обработки, программ и баз данных. 2.2. Управление доступом к информации. 2.3. . Парольная идентификация и аутентификация в сетевых операционных системах. 2.4. Международное нормативно-правовое регулирование защиты информации.

лабораторная работа (4 часа(ов)):

Отчет по лабораторной работе.

Тема 3. Информационные и компьютерные преступления как объекта защиты

лекционное занятие (4 часа(ов)):

3.1 Понятие об информационных и компьютерных преступлениях. 3.2. Уголовно-правовая характеристика преступлений в сфере компьютерной информации. 3.3. . Основные положения закона "Об информации, информатизации и защите информации"

лабораторная работа (2 часа(ов)):

Отчет по лабораторной работе.

Тема 4. Виды кодирования и их использование в защите информации

лекционное занятие (4 часа(ов)):

4.1.Криптографические средства защиты информации 4.2. Алгоритмы симметрического и асимметрического шифрования 4.3 сертификат открытого ключа 4.3. Математические основы современной криптологии. 4.4. Функции Хэширования

лабораторная работа (2 часа(ов)):

Отчет по лабораторной работе.

Тема 5. Обеспечение конфиденциальности и целостности информационных ресурсов

лекционное занятие (2 часа(ов)):

5.1.Шифрования конфиденциальных ресурсов для разграничения доступа к ним. 5.2. обеспечения целостности информационных ресурсов с помощью механизма электронной цифровой подписи.

лабораторная работа (2 часа(ов)):

Отчет по лабораторной работе.

Тема 6. Лабораторная работа №1 Разграничение прав пользователей в защищенных версиях операционной системы Windows

лекционное занятие (2 часа(ов)):

Разграничение прав пользователей в защищенных версиях операционной системы Windows.

лабораторная работа (2 часа(ов)):

Лабораторная работа №1 Разграничение прав пользователей в защищенных версиях операционной системы Windows

Тема 7. Лабораторная работа №2 Реализация политики безопасности в защищенных версиях операционной системы Windows

лекционное занятие (4 часа(ов)):

Реализация политики безопасности в защищенных версиях операционной системы Windows.

лабораторная работа (4 часа(ов)):

Лабораторная работа №2 Реализация политики безопасности в защищенных версиях операционной системы Windows

Тема 8. Лабораторная работа №3 Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows

лекционное занятие (2 часа(ов)):

Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows.

лабораторная работа (2 часа(ов)):

Лабораторная работа №3 Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows

Тема 9. Лабораторная работа №4 Освоение средств защищенных версий операционной системы Windows, предназначенных для ? разграничения доступа субъектов к принтерам; ? разграничения доступа к разделам реестра; ? обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы.

лекционное занятие (2 часа(ов)):

Освоение средств защищенных версий операционной системы Windows, предназначенных для разграничения доступа субъектов к принтерам; для разграничения доступа к разделам реестра; для обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы.

лабораторная работа (4 часа(ов)):

Лабораторная работа №4 Освоение средств защищенных версий операционной системы Windows, предназначенных для ? разграничения доступа субъектов к принтерам; ? разграничения доступа к разделам реестра; ? обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы.

Тема 10. Лабораторная работа № 5 Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов

лекционное занятие (2 часа(ов)):

Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов.

лабораторная работа (2 часа(ов)):

Лабораторная работа № 5 Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов

Тема 11. Лабораторная работа №6 Определение правил для выбора защищенного пароля, определение слабо защищенного пароля, методы подбора пароля

лекционное занятие (2 часа(ов)):

Определение правил для выбора защищенного пароля, определение слабо защищенного пароля, методы подбора пароля.

лабораторная работа (2 часа(ов)):

Лабораторная работа №6 Определение правил для выбора защищенного пароля, определение слабо защищенного пароля, методы подбора пароля

Тема 12. Лабораторная работа №7 Способы шифрования (дешифрования) или хеширования паролей

лекционное занятие (2 часа(ов)):

Способы шифрования (дешифрования) или хеширования паролей.

лабораторная работа (4 часа(ов)):

Лабораторная работа №7 Способы шифрования (дешифрования) или хеширования паролей.

Тема 13. Лабораторная работа №8 Создание комплексной защиты информации

лекционное занятие (2 часа(ов)):

Создание комплексной защиты информации.

лабораторная работа (2 часа(ов)):

Лабораторная работа №8

Тема 14. Лабораторная работа №9 Система фильтрации IP-трафика

лекционное занятие (2 часа(ов)):

Система фильтрации IP-трафика.

лабораторная работа (2 часа(ов)):

Лабораторная работа №9

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. Свойства информации как объекта защиты	7	2	- подготовку к выполнению лабораторного практикума;	4	- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов;
2.	Тема 2. Методы контроля доступа к информации и ее инженерно-техническая защита	7	2	- подготовку к выполнению лабораторного практикума;	6	- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов;
3.	Тема 3. Информационные и компьютерные преступления как объекта защиты	7	2	- подготовку к выполнению лабораторного практикума;	6	- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов;
4.	Тема 4. Виды кодирования и их использование в защите информации	7	2	- подготовку к выполнению лабораторного практикума;	6	- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов;
5.	Тема 5. Обеспечение конфиденциальности и целостности информационных ресурсов	7	1	- подготовку к выполнению лабораторного практикума;	2	- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов;

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
6.	Тема 6. Лабораторная работа ◆1 Разграничение прав пользователей в защищенных версиях операционной системы Windows	7	2	- подготовку к выполнению лабораторного практикума;	6	- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов;
7.	Тема 7. Лабораторная работа ◆2 Реализация политики безопасности в защищенных версиях операционной системы Windows	7	2	- подготовку к выполнению лабораторного практикума;	8	- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов;
8.	Тема 8. Лабораторная работа ◆3 Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows	7	2	- подготовку к выполнению лабораторного практикума;	4	- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов;
9.	Тема 9. Лабораторная работа ◆4 Освоение средств защищенных версий операционной системы Windows, предназначенных для ? разграничения доступа субъектов к принтерам; ? разграничения доступа к разделам реестра; ? обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы.	7	2	- подготовку к выполнению лабораторного практикума;	6	- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов;
10.	Тема 10. Лабораторная работа ◆ 5 Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов	7	2	- подготовку к выполнению лабораторного практикума;	6	- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов;

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
11.	Тема 11. Лабораторная работа №6 Определение правил для выбора защищенного пароля, определение слабо защищенного пароля, методы подбора пароля	7	2	- подготовку к выполнению лабораторного практикума;	4	- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов;
12.	Тема 12. Лабораторная работа №7 Способы шифрования (дешифрования) или хеширования паролей	7	2	- подготовку к выполнению лабораторного практикума;	4	- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов;
13.	Тема 13. Лабораторная работа №8 Создание комплексной защиты информации	7	2	- подготовку к выполнению лабораторного практикума;	6	- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов;
14.	Тема 14. Лабораторная работа №9 Система фильтрации IP-трафика	7	2	- подготовку к выполнению лабораторного практикума;	4	- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов.
	Итого				72	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекционных и лабораторных занятий, а также самостоятельной работы студентов.

Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель-формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи зачета минимум и дополнительная литература.

Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать утверждения.

Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы.

Кроме того, самостоятельная работа включает подготовку к экзамену. При подготовке к сдаче экзамена весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки.

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

Тема 1. Свойства информации как объекта защиты

- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов; , примерные вопросы:

Основные положения теории защиты информации. Сущность проблемы и задачи защиты информации в информационных и телекоммуникационных сетях.

Тема 2. Методы контроля доступа к информации и ее инженерно-техническая защита

- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов; , примерные вопросы:

Традиционные и нетрадиционные меры и методы защиты информации. Криптографические методы и средства защиты информации. Информационная безопасность предприятия.

Тема 3. Информационные и компьютерные преступления как объекта защиты

- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов; , примерные вопросы:

Информационные и компьютерные преступления как объекта защиты.

Тема 4. Виды кодирования и их использование в защите информации

- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов; , примерные вопросы:

Методы сохранения конфиденциальности, целостности информации и работоспособности информационно-вычислительных систем.

Тема 5. Обеспечение конфиденциальности и целостности информационных ресурсов

- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов; , примерные вопросы:

обеспечение отказоустойчивости (резервирование, дублирование, зеркалирование оборудования и данных, например через использование RAID-массивов); обеспечение безопасного восстановления (резервное копирование и электронное архивирование информации); криптографическая защита информации (шифрование, хеширование, электронная цифровая подпись).

Тема 6. Лабораторная работа №1 Разграничение прав пользователей в защищенных версиях операционной системы Windows

- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов; , примерные вопросы:

Разграничение прав пользователей в защищенных версиях операционной системы Windows.

Тема 7. Лабораторная работа №2 Реализация политики безопасности в защищенных версиях операционной системы Windows

- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов; , примерные вопросы:

Реализация политики безопасности в защищенных версиях операционной системы Windows.

Тема 8. Лабораторная работа №3 Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows

- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов; , примерные вопросы:

Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows.

Тема 9. Лабораторная работа №4 Освоение средств защищенных версий операционной системы Windows, предназначенных для ? разграничения доступа субъектов к принтерам; ? разграничения доступа к разделам реестра; ? обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы.

- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов; , примерные вопросы:

Освоение средств защищенных версий операционной системы Windows, предназначенных для: - разграничения доступа субъектов к принтерам; - разграничения доступа к разделам реестра; - обеспечения конфиденциальности папок и файлов с помощью шифрующей файловой системы.

Тема 10. Лабораторная работа № 5 Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов

- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов; , примерные вопросы:

Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов.

Тема 11. Лабораторная работа №6 Определение правил для выбора защищенного пароля, определение слабо защищенного пароля, методы подбора пароля

- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов; , примерные вопросы:

Определение правил для выбора защищенного пароля, определение слабо защищенного пароля, методы подбора пароля.

Тема 12. Лабораторная работа №7 Способы шифрования (дешифрования) или хеширования паролей

- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов; , примерные вопросы:

Способы шифрования (дешифрования) или хеширования паролей.

Тема 13. Лабораторная работа №8 Создание комплексной защиты информации

- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов; , примерные вопросы:

Создание комплексной защиты информации.

Тема 14. Лабораторная работа №9 Система фильтрации IP-трафика

- изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов. , примерные вопросы:

Система фильтрации IP-трафика.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

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

7.1. Основная литература:

1. Девянин П.Н. Модели безопасности компьютерных систем: Уч. Пособие для студентов ВУЗов. - М.: Издательский центра "Академия", 2005.

2. Мельников В.П. Информационная безопасность и защита информации; учеб.пособие для студентов высш.учеб.заведений/ Мельников В.П., Клейменов С.А., Петраков А.М.; под ред. Мельникова В.П. М.: Издательский центра "Академия", 2008.

3. Олифер В.Г. , Н.А. Олифер. Компьютерные сети. Принципы, технологии, протоколы. СПб.: "Piter-press", 2001, 668 с.

4. Расторгуев С.П. Программные методы защиты информации. Пенза, 2000, 100 с.

5. Макнамара Д. Секреты компьютерного шпионажа: Тактика и контрмеры. /Пер. с англ.; Под ред. С.М. Молявко. - М.: БИНОМ. Лаборатория знаний, 2004. - 536 с.

6.Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. Справочное пособие - СПб.: БХВ - Петербург, Арлит, 2002. - 496 с.

Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и защита - М.: ДМК Пресс, 2008. - 544 с.

7. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. - СПб.: Наука и Техника, 2004. - 384 с.

7.2. Дополнительная литература:

1. Герасименко В.А., Малюк А.А. "Основы защиты информации" М.: МИФИ. /Учебник (рекомендован Минобразованием России в качестве учебника для студентов вузов). 1997 - 538 с.

2. Бакланов В.В. Информационные модели человека-нарушителя: лекция. /В. В. Бакланов; в/ч 69617. Екатеринбург, 1996. - 77 с.

3. Малюк А.А., Пазизин С.В., Погожин Н.С. "Введение в защиту информации в автоматизированных системах" М.: "Горячая Линия-Телеком". 2001 - 148 с.

4. Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации. М.: Издательская группа "Юрист", 2001 - 415с.

5. Ярочкин В.И. "Информационная безопасность". М.: "Международные отношения". 2000 - 400 с.

нормативно-правовые акты:

1. ФЗ "Об информации, информационных технологиях и защите информации", № 149-ФЗ от 27.07.2006.

2. ФЗ "О персональных данных", № 152-ФЗ от 27.07.2006.

7.3. Интернет-ресурсы:

Lan Agent - мониторинг компьютеров ЛС - http://www.lanagent.ru/

Википедия - http://ru.wikipedia.org/

Интеллект-сервис - http://www.it-ic.ru/

Стандарты информационной безопасности - http://www.arinteg.ru/articles/standarty-informatsionnoy-bezopasnosti-27697.html

Школа IT-менеджмента - http://www.itmane.ru/mba-cso

8. Материально-техническое обеспечение дисциплины(модуля)

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

Лекционные занятия по дисциплине проводятся в аудитории, оснащенной проекционным оборудованием. Лабораторные занятия проводятся в специализированных компьютерных кабинетах кафедры информатики и вычислительных технологий с выходом в Интернет и установленной интерактивной доской.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 230700.62 "Прикладная информатика" и профилю подготовки Прикладная информатика в экономике .

Автор(ы):
Гайнутдинова Т.Ю. _____
"__" _____ 201 __ г.

Рецензент(ы):
Хакимов Р.Г. _____
"__" _____ 201 __ г.