

**МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
КРАСНОДАРСКИЙ УНИВЕРСИТЕТ**

ЧАСТНАЯ МЕТОДИКА

дисциплина

“ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ”

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
1. Общая характеристика целей и задач дисциплины, ее особенностей	4
2. Характеристика частной методики, ее структура	6
3. Рекомендации по использованию частной методики в практической деятельности преподавателя	9
4. Краткие сведения об авторах	10
II. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРЕПОДАВАНИЮ И ИЗУЧЕНИЮ ДИСЦИПЛИНЫ	11
1. Тематические планы дисциплины	11
2. Общие методические рекомендации по преподаванию дисциплины	13
3. Методические разработки аудиторных занятий	14
3.1. Цели и задачи занятия	14
3.2. Рекомендации по структуре (плану) занятия	17
3.3. Рекомендации по оборудованию занятия	19
3.4. Методические рекомендации по повторению, закреплению и контролю знаний, умений, навыков учащихся, полученных на предыдущих занятиях	20
3.5. Методические рекомендации по изучению, закреплению и контролю усвоения нового материала	25
3.6. Методические рекомендации по постановке задания к следующему занятию, по организации самостоятельной работы учащихся	28
4. Методические указания по изучению дисциплины (для обучающихся)	30
Приложение 1. Структурно-логическая схема изучения дисциплины	33
Приложение 2. Перечень примерных вопросов (заданий) для самостоятельной работы обучающихся	34
Приложение 3. Примерный перечень вопросов (заданий) для проведения рубежного контроля.	36
Приложение 4. Примерный перечень вопросов для проведения промежуточной аттестации с рекомендациями по подготовке к зачету	38

Приложение 5. Учебно-методическое обеспечение дисциплины	40
Приложение 6. Перечень мультимедийного сопровождения лекционных занятий	42
Приложение 7. Перечень компьютерных обучающих программ	43

ВВЕДЕНИЕ

1. Общая характеристика целей и задач дисциплины, ее особенностей

Дисциплина «Информационная безопасность» является общеобразовательной дисциплиной, формирующей теоретические и практические аспекты, касающиеся применения технологий защиты информации в профессиональной деятельности.

Целью изучения дисциплины «Информационная безопасность» является приобретение курсантами и слушателями теоретических знаний, практических умений и навыков применения современных информационных технологий для использования в профессиональной деятельности по защите информации и расследования компьютерных преступлений.

Задачами дисциплины является формирование у обучаемых общего представления о современных концепциях информационной безопасности, знакомство с различными методами защиты информации от несанкционированного доступа, изучение криптографических средств, как основного инструмента обеспечения сохранности компьютерной информации, приобретение практических навыков работы с современными аппаратными и программными средствами защиты информации.

Особенностью преподавания дисциплины «Информационная безопасность» является создание в учебном процессе специальных организационно-методических и программно-технических условий, благоприятствующих усвоению необходимых знаний, умений и навыков на уровне современных требований, а именно:

оборудование компьютерных лабораторий достаточным количеством современной компьютерной техники;

установку соответствующего содержанию дисциплины информационного и программного обеспечения;

использование современных информационных технологий обучения.

В результате изучения дисциплины выпускники должны:

иметь представление:

- о сущности, содержании информационной безопасности;
- о месте, роли и тенденциях развития методов и технологий защиты компьютерной информации,
- об особенностях и проблемах защиты информации в правоохранительной деятельности;

знать:

- фундаментальные понятия информационной безопасности;
- основные принципы, правила хранения, передачи и защиты компьютерной правовой информации;
- состав, функции и конкретные возможности аппаратно-программного обеспечения в процессе решения задач профессионально-служебной деятельности;
- основные нормативные документы, законы и указы Президента, регламентирующие организацию защиты информации;

уметь:

- использовать современные аппаратно-программные средства в области защиты информации;
- грамотно управлять системой защиты информации при работе на персональном компьютере;
- выявлять и классифицировать источники внешних и внутренних угроз;
- защищать информационные ресурсы от вредоносного программного обеспечения;

иметь навыки:

- использования основных защитных механизмов, мер и средств обеспечения информационной безопасности;
- применения комплексного подхода к построению системы защиты информации;
- использования криптографических методов защиты информации.

2. Характеристика частной методики, ее структура

Частная методика преподавания учебной дисциплины «Информационная безопасность» является комплексным организационно-методическим документом кафедры, в котором изложен единый (примерный) взгляд кафедры на методику преподавания данной дисциплины и обобщен передовой опыт профессорско-преподавательского состава в проведении всех учебных занятий, предусмотренных учебной программой.

Частная методика дополняет и конкретизирует тематический план изучения дисциплины «Информационная безопасность» и является основным документом для подготовки преподавателей к занятиям и важным средством совершенствования их методического мастерства.

Частность предлагаемой методики по дисциплине «Информационная безопасность» заключается в гибком сочетании традиционных методов обучения с инновационными образовательными технологиями. Структура частной методики (ЧМ) включает в себя три взаимосвязанных и взаимопроникающих компонента: познавательная деятельность обучаемого (ПД), мотивационный компонент (М), управление этой деятельностью (УД) со стороны педагога и технических средств обучения. Символически это описывается следующей условной формулой:

$$\text{ЧМ}=\text{ПД}+\text{М}+\text{УД}.$$

Рассмотрим более подробно компоненты входящие в предлагаемую методику и обеспечивающую ее частность.

Лекция-визуализация. Лекция-визуализация выступает как результат поиска новых возможностей реализации принципа наглядности. Психолого-педагогические исследования показывают, что наглядность не только способствует более успешному восприятию и запоминанию учебного материала, но и позволяет проникнуть глубже в существо познаваемых явлений. Это происходит за счет работы обоих полушарий, а не одного левого, логического, привычно работающего при освоении точных наук. Правое полушарие, отвечающее за

образно-эмоциональное восприятие предъявляемой информации, начинает активно работать именно при ее визуализации. Визуализация лекционных занятий происходит за счет разработки мультимедийных презентаций (Приложение. 6) в форматах ppt и pdf. Все разрабатываемые презентации удовлетворяют основным требованиям, выдвигаемым к такому типу методического обеспечения:

1. Минимизация текстовой информации за счет использования структурных схем, списков и т.д.
2. Наличие анимационных эффектов.
3. Цветовое оформление слайдов.
4. Использование достаточно крупного шрифта (учитывается специфика той аудитории, в которой будет демонстрироваться презентация).
5. Импорт дополнительных объектов: графика, аудио, видео.

Индивидуальные тестовые задания. Разработанная частная методика сводится не только к приобретению обучаемыми определенных знаний и навыков, но и овладению приемами самостоятельного приобретения знаний и их применения. Решению проблемы индивидуального обучения способствует выполнение *индивидуальных тестовых заданий*, позволяющее при разноуровневом обучении оценить знания учащихся. *Тестовый контроль* – это такой вид контроля, при котором обеспечены равные для всех обучаемых объективные условия проверки. Тестовые задания классифицируют по форме их строения:

- тесты с конструированными ответами;
- тесты с выборочными ответами.

Тесты с конструированными ответами представляют собой компьютерные обучающие программы (Приложение 7) разработанные на языке программирования Visual Basic for Application (VBA) для программной среды MS Excel. Процесс генерации заданий и последующей их проверки полностью автоматизирован. Самое ценное в данном компоненте – структура заданий и подбор задач. Тип компьютера, операционной системы играет второстепенное значение, хотя, чем шире возможности компьютера, тем больше эффективность приме-

няемой технологии. Для данного вида тестов характерно то, что обучаемые сами составляют короткие однозначные ответы и вводят их в соответствующие ячейки рабочего листа.

Тесты с выборочными ответами дают возможность быстрее усваивать все виды явлений, лучше понимать их общие и отличительные качества, легче их классифицировать. Большинство технических средств контроля ориентировано на применение именно тестовых заданий с выборочными ответами. Этот метод вносит разнообразие в учебный процесс, повышает интерес к предмету, способствуя тем самым лучшему усвоению знаний. Тесты с выборочными ответами разработаны в автоматизированной контролирующей системе (АКС) проверки знаний Контроль10. АКС Контроль10 представляет собой программный продукт, в котором преподаватель создает тему своей предметной области и в этой теме создает предметно-ориентированный тест. В тестах имеется возможность использовать различные типы вопросов: текстовые, графические, звуковые, вопросы с использованием видеофрагментов. Количество тем, вопросов и тестов в данной системе неограниченно и может регулироваться разработчиком темы и находящихся в них тестов. Ограничение на количество тем и содержащихся в них тестов может накладывать лишь дисковое пространство используемого жесткого диска. По своему желанию разработчик тестов может установить пароль на запуск теста или пароль на возможность администрирования (редактирования) ранее введенных данных.

Сам процесс тестирования предполагает работу с человеком в диалоговом режиме, то есть в режиме прямой и обратной связи. Компьютер "задает вопрос", выводя его на экран, тестируемый отвечает на него, выделяя верный на свой взгляд вариант ответа (верных вариантов ответа может быть несколько) с помощью клавиатуры или мыши. При этом на экране в строке состояния выводится вся текущая информация необходимая пользователю для корректировки своих действий: верный/неверный ответ, время оставшееся до окончания теста, количество выбранных вопросов, количество верных ответов и т.д.

Необходимыми и достаточными условиями реализации частной методики являются:

- оснащение лекционной аудитории техническими средствами обучения: персональный компьютер, мультимедийный проектор, проекционный экран;
- проведение практических занятий в компьютерной лаборатории, с обязательным оснащением каждого обучаемого автоматизированным рабочим местом;
- наличие у преподавателя и обучаемых начальных навыков работы с операционной средой персонального компьютера, прикладным программным обеспечением.

Важным принципом разработанной частной методики также выступает принцип целостности. Принцип целостности заключается в достижении гармоничного взаимодействия всех элементов частной методики. При этом недопустимо внесение изменений в один из элементов частной методики, не затрагивая соответствующей перестройкой другие. Например, при изменении цели, неизбежна трансформация содержания частной методики и процессов обучения таким образом, чтобы они способствовали достижению поставленных целей.

3. Рекомендации по использованию частной методики в практической деятельности преподавателя

Данная частная методика предназначена для профессорско-преподавательского состава кафедры задействованного в учебном процессе для преподавания дисциплины «Информационная безопасность». В практической деятельности данная частная методика используется для полного и качественного планирования проведения каждого вида занятия по преподаваемой дисциплине и единства понимания структуры учебного материала.

Использование частной методики для подготовки к занятиям рекомендуется осуществлять в следующей последовательности:

уточнение, согласно тематического плана, темы и вида занятия;

уточнение соответствующих компетенций (знаний, умений и навыков) формируемых у курсантов в ходе проведения конкретного занятия.

уточнение цели и задачи занятия в соответствии с темой, видом занятия, и формируемыми компетенциями.

формирование структуры (плана) занятия

организация оборудования занятия исходя из темы и целей занятия;

уточнение вопросов по повторению, закреплению и контролю знаний, умений и формируемых навыков, полученных на предыдущих занятиях;

уточнение состава учебных вопросов по изучению, закреплению и контролю усвоения нового материала;

разработка задания к следующему занятию и рекомендаций по организации самостоятельной работы курсантов.

4. Краткие сведения об авторах

Фамилия, имя, отчество: Старостенко Игорь Николаевич

Должность: начальник кафедры информатики и математики

Специальное звание: майор милиции

Ученая степень: кандидат физико-математических наук

Сфера научных интересов: информационно-технические средства, защита информации, механика деформируемого твердого тела, компьютерные технологии в образовательном процессе.

II. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРЕПОДАВАНИЮ И ИЗУЧЕНИЮ ДИСЦИПЛИНЫ

1. Тематические планы дисциплины

Примерный тематический план

*очная форма обучения на базе среднего (полного) общего образования, срок
обучения 5 лет*

№ п/п	НАИМЕНОВАНИЕ ЧАСТЕЙ, РАЗДЕЛОВ И ТЕМ	ВСЕГО	ЧАСЫ		КОЛИЧЕСТВО ЧАСОВ ПО ВИДАМ ЗАНЯТИЙ			
			Аудиторные	Самостоятельные	Лекции	Семинарские за- нятия	Практ. занятия / контр.раб.	другие
1	Концепции информационной безопасности	6	4	2	2		2	
2	Методы и средства защиты информации	6	4	2	2		2	
3	Криптографические методы защиты информации	10	8	2	2		6	
4	Аппаратные и программные средства защиты компьютерной информации	8	6	2	2		4	
5	Безопасность компьютерных сетей	6	4	2	2		2	
	Зачет	4	4					4
	Итого	40	30	10	10		16	4

Примерный тематический план

заочная форма обучения на базе среднего (полного) общего образования, срок обучения 6 лет

№ п/п	НАИМЕНОВАНИЕ ЧАСТЕЙ, РАЗДЕЛОВ И ТЕМ	ВСЕГО	ЧАСЫ		КОЛИЧЕСТВО ЧАСОВ ПО ВИДАМ ЗАНЯТИЙ			
			Аудиторные	Самостоятельные	Лекции	Семинарские занятия	Практ. занятия / контр. раб.	Другие
1	Концепции информационной безопасности	6	2	4	2			
2	Методы и средства защиты информации	6		6				
3	Криптографические методы защиты информации	10	2	8			2	
4	Аппаратные и программные средства защиты компьютерной информации	8		8				
5	Безопасность компьютерных сетей	6		6				
	Зачет	4	4					4
	Итого	40	8	32	2		2	4

Примерный тематический план
заочная форма обучения на базе среднего профессионального образования,
срок обучения 4 года

№ п/п	НАИМЕНОВАНИЕ ЧАСТЕЙ, РАЗДЕЛОВ И ТЕМ	ВСЕГО	ЧАСЫ		КОЛИЧЕСТВО ЧАСОВ ПО ВИДАМ ЗАНЯТИЙ			
			Аудиторные	Самостоятельные	Лекции	Семинарские за- нятия	Практ. занятия / контр.раб.	Другие
1	Концепции информационной безопасности	6	2	4	2			
2	Методы и средства защиты информации	6		6				
3	Криптографические методы защиты информации	10	2	8			2	
4	Аппаратные и программные средства защиты компьютерной информации	8		8				
5	Безопасность компьютерных сетей	6		6				
	Зачет	4	4					4
	Итого	40	8	32	2		2	4

2. Общие методические рекомендации по преподаванию дисциплины

В целях реализации учебной программы преподавателю предоставлено право выбора и использования методик обучения, учебников, учебных пособий и методов оценки знаний.

Для изучения с курсантами дисциплины «Информационная безопасность» используются компьютерные классы вычислительного центра университета, где в соответствии с расписанием занятий преподавателем проводятся лекционные и практические занятия. Занятия в компьютерном классе предполагают индивидуально-групповое изучение основ информационной безопасности и защиты информации.

Дисциплина состоит из пяти тем. Первые две темы раскрывают теоретические и правовые основы информационной безопасности. Третья тема посвящена криптографии – самому мощному инструменту защиты информации. Четвертая и пятая темы носят практическую направленность и охватывают все основные аспекты обеспечения безопасности информационных ресурсов, в том числе при работе в локальных и глобальных компьютерных сетях. Общий объем дисциплины составлен из расчета учебного времени 40 часов. Бюджет времени определен с учетом времени, отводимого учебным планом Краснодарского университета МВД России на дисциплину «Информационная безопасность» при различных формах обучения для цикла общематематических и естественнонаучных дисциплин. Изучение дисциплины завершается сдачей зачета.

3. Методические разработки аудиторных занятий

3.1. Цели и задачи занятия

Тема № 1. Концепции информационной безопасности

Лекция

Цель занятия: дать понятия информации, информационной безопасности, защиты информации. Рассмотреть общие концептуальные положения информационной безопасности, основные этапы обеспечения защиты информации: определение политики информационной безопасности, управление рисками, аудит информационной безопасности.

Практическое занятие № 1

Цель занятия: изучение общей концепции информационной безопасности, структуры и направления обеспечения сохранности информации.

Задачи занятия: рассмотреть основные концептуальные положения системы защиты информации, нормативно-правовые документы, регламентирующие отношения в сфере информационной безопасности.

Тема № 2. Методы и средства защиты информации

Лекция

Цель занятия: Рассмотреть основные угрозы и характеристики информации. Определить и классифицировать методы и средства защиты информации. Обозначить средства обеспечения безопасности при работе в глобальной сети

	Internet.
Практическое занятие № 1	<p>Задачи занятия:</p> <p>Цель занятия: изучение общей классификации методов и средств защиты информации от различного вида угроз.</p> <p>Задачи занятия: рассмотреть основные типы угроз и характеристики информации, определить основные уровни защиты информационных ресурсов, рассмотреть принципы обеспечения сохранности информации глобальной сети Интернет</p>
	Тема № 3. Криптографические методы защиты информации
Лекция	<p>Цель занятия: Ввести базовые понятия криптографии. Рассмотреть классификацию криптоалгоритмов. Определить анализ стойкости криптографических примитивов.</p> <p>Задачи занятия:</p>
Практическое занятие № 1	<p>Цель занятия: изучение основных положений криптографических методов и средств защиты информации.</p> <p>Задачи занятия: рассмотреть способы зашифрования и расшифрования информации с использованием различных криптоалгоритмов.</p>
Практическое занятие № 2	<p>Цель занятия: изучение основных положений криптографических методов и средств защиты информации.</p> <p>Задачи занятия рассмотреть способы зашифрования и расшифрования информации с использованием различных криптоалгоритмов.</p>
Практическое занятие № 3	<p>Цель занятия: изучение основных положений криптографических методов и средств защиты информации.</p> <p>Задачи занятия рассмотреть методы анализа одноалфавитных и многоалфавитных систем.</p>
	Тема № 4. Аппаратные и программные средства защиты компьютерной информации
Лекция	<p>Цель занятия: Определить и классифицировать аппаратные и программные средства защиты информации. Рассмотреть аппаратные и программные средства защиты в реализации Microsoft.</p> <p>Задачи занятия:</p>
Практическое занятие № 1	<p>Цель занятия: изучение основных положений аппаратно-программных методов и средств за-</p>

щиты компьютерной информации от вредоносного программного обеспечения.

Задачи занятия: рассмотреть источники и распространение угроз, проанализировать состав и функциональное назначение каждого отдельного компонента антивирусных программ: файловый антивирус, почтовый антивирус, веб-антивирус, анти-шпион, анти-спам, межсетевой экран.

Практическое занятие № 2

Цель занятия: изучение основных положений аппаратных и программных средств защиты компьютерной информации.

Задачи занятия: рассмотреть криптографические, стеганографические утилиты защиты компьютерной информации, проанализировать алгоритм установки парольной защиты средствами операционной системы.

Тема № 5. Безопасность компьютерных сетей

Лекция

Цель занятия: Рассмотреть основные аспекты безопасности компьютерных сетей, изучить технологии и принципы функционирования межсетевых экранов.

Практическое занятие № 1

Цель занятия: изучить основные аспекты безопасности компьютерных сетей, технологии и принципы функционирования межсетевых экранов.

Задачи занятия: рассмотреть классификацию сетевых атак по цели: серверы, рабочие станции, среды передачи информации, узлы коммутации сетей; изучить различные виды межсетевых экранов: межсетевые экраны уровня соединения, межсетевые экраны прикладного уровня, межсетевые экраны с динамической фильтрацией пакетов, межсетевые экраны инспекции состояний, межсетевые экраны уровня ядра, персональные межсетевые экраны, распределенные межсетевые экраны.

3.2. Рекомендации по структуре (плану) занятия

Тема № 1. Концепции информационной безопасности

- | | |
|--------------------------|---|
| Лекция | <ol style="list-style-type: none">1. Понятие информационной безопасности. Общая концептуальная модель защиты информации2. Политика безопасности3. Управление рисками4. Аудит системы управления информационной безопасностью |
| Практическое занятие № 1 | <ol style="list-style-type: none">1. Концептуальная модель информационной безопасности.2. Основные направления защиты информации. Правовое обеспечение информационной безопасности.3. Защита информации с точки зрения теории рисков. |

Тема № 2. Методы и средства защиты информации

- | | |
|--------------------------|---|
| Лекция | <ol style="list-style-type: none">1. Угрозы безопасности2. Характеристики информации3. Общая классификация методов и средств защиты информации4. Методы решения задач информационной безопасности5. Средства обеспечения информационной безопасности в Internet |
| Практическое занятие № 1 | <ol style="list-style-type: none">1. Классификация угроз информации.2. Характеристики информации.3. Законодательные, административные и технические методы и средства защиты информации.4. Анализ средств обеспечения безопасности информации при работе в Интернет. |

Тема № 3. Криптографические методы защиты информации

- | | |
|--------------------------|---|
| Лекция | <ol style="list-style-type: none">1. Понятие криптографии2. Криптографические примитивы3. Классификация криптоалгоритмов4. Стандарты шифрования5. Симметричные криптосистемы6. Анализ стойкости криптографических примитивов |
| Практическое занятие № 1 | <ol style="list-style-type: none">1. Зашифрование и расшифрование информации с помощью шифра Цезаря2. Зашифрование и расшифрование информации с помощью шифра Гронсфельда |

3. Зашифрование и расшифрование информации с помощью шифра Виженера
4. Зашифрование и расшифрование информации с помощью шифра Хилла
- Практическое занятие № 2
1. Зашифрование и расшифрование информации с помощью шифра Цезаря
2. Зашифрование и расшифрование информации с помощью шифра Гронсфельда
3. Зашифрование и расшифрование информации с помощью шифра Виженера
4. Зашифрование и расшифрование информации с помощью шифра Хилла
- Практическое занятие № 3
1. Методы анализа одноалфавитных систем шифрования
- а) Частотный анализ
- б) Метод полосок
2. Методы анализа многоалфавитных систем шифрования
- а) Сведение к анализу одноалфавитных систем
- б) Метод Казиски
- Тема № 4. Аппаратные и программные средства защиты компьютерной информации
- Лекция
1. Защита данных
- 1.1. Шифрование дисков
- 1.2. Архивация с шифрованием
2. Аппаратные и программные средства защиты в реализации Microsoft
3. Комплексный подход к построению системы защиты информации
4. Навесные защиты (протекторы).
- Практическое занятие № 1
1. Источники угроз: человеческий фактор, технический фактор, стихийный фактор.
2. Распространение угроз: интернет, интранет, электронная почта, съемные носители информации.
3. Компоненты постоянной защиты: файловый антивирус, почтовый антивирус, веб антивирус, проактивная защита, анти-шпион, сетевой экран, анти-спам.
- Практическое занятие № 2
1. Защита компьютерной информации с помощью скрытых виртуальных логических дисков.
2. Шифрование файлов и папок с помощью различных криптоалгоритмов.
3. Удаление информации без возможности ее

восстановления, менеджер паролей.

	Тема № 5. Безопасность компьютерных сетей
Лекция	1. Серверы 2. Рабочие станции 3. Среда передачи информации 4. Узлы коммутации сетей 5. Технологии межсетевых экранов
Практическое занятие № 1	1. Защита компьютерной информации с помощью скрытых виртуальных логических дисков. 2. Шифрование файлов и папок с помощью различных криптоалгоритмов. 3. Удаление информации без возможности ее восстановления, менеджер паролей.

3.3. Рекомендации по оборудованию занятия

	Тема № 1. Концепции информационной безопасности
Лекция	Компьютерная учебная лаборатория, видеопроектор, мультимедийная презентация «Концепции информационной безопасности».
Практическое занятие № 1	Компьютерная учебная лаборатория, видеопроектор, учебно-методический материал в электронном виде.
	Тема № 2. Методы и средства защиты информации
Лекция	Компьютерная учебная лаборатория, видеопроектор, учебно-методический материал в электронном виде.
Практическое занятие № 1	Компьютерная учебная лаборатория, видеопроектор, учебно-методический материал в электронном виде, программный комплекс «Методы и средства защиты информации».
	Тема № 3. Криптографические методы защиты информации
Лекция	Компьютерная учебная лаборатория, видеопроектор, учебно-методический материал в электронном виде.
Практическое занятие № 1	Компьютерная учебная лаборатория, видеопроектор, учебно-методический материал в электронном виде, программный комплекс «Криптографические методы защиты информации».
Практическое занятие № 2	Компьютерная учебная лаборатория, видеопроектор, учебно-методический материал в электронном виде, программный комплекс «Криптографические методы защиты информации».

Практическое занятие № 3 Компьютерная учебная лаборатория, видеопроектор, учебно-методический материал в электронном виде, программный комплекс «Криптографические методы защиты информации».

Тема № 4. Аппаратные и программные средства защиты компьютерной информации

Лекция Компьютерная учебная лаборатория, видеопроектор, учебно-методический материал в электронном виде.

Практическое занятие № 1 Компьютерная учебная лаборатория, видеопроектор, учебно-методический материал в электронном виде, программный комплекс «Аппаратные и программные средства защиты компьютерной информации».

Практическое занятие № 2 Компьютерная учебная лаборатория, видеопроектор, учебно-методический материал в электронном виде, программный комплекс «Аппаратные и программные средства защиты компьютерной информации».

Тема № 5. Безопасность компьютерных сетей

Лекция Компьютерная учебная лаборатория, видеопроектор, учебно-методический материал в электронном виде.

Практическое занятие № 1 Компьютерная учебная лаборатория, видеопроектор, учебно-методический материал в электронном виде, программный комплекс «Безопасность компьютерных сетей».

3.4. Методические рекомендации по повторению, закреплению и контролю знаний, умений, навыков учащихся, полученных на предыдущих занятиях

Для повторения, закрепления и контроля знаний, умений, навыков учащихся, полученных на предыдущих занятиях следует выполнить следующие практические задания.

ТЕМА №1. Концепции информационной безопасности

Практическое занятие №1

1. Для шифрования информации был использован код, состоящий из 8192 различных знаков. Какое количество байт содержит шифровка, состоящая из 61 групп по 350 знаков в каждой группе?

2. Шифровка состояла из 2048 групп символов по 16384 символов в группе и содержала 54525952 байт информации. С помощью скольких различных знаков была закодирована шифровка?
3. В доме 595 квартир(ы). Сколько бит должно содержать двоичное слово, чтобы закодировать в этом доме все квартиры?
4. Даны два текста, содержащих одинаковое количество символов. Первый текст состоит из алфавита мощностью 32 символов, а второй текст - из 1024 символов. Во сколько раз информации во втором тексте больше чем в первом?
5. Информационное сообщение передается в течении 20 минут со скоростью 80 байт в секунду. Сколько символов содержало данное сообщение, если был использован алфавит из 256 символов?
6. При угадывании целого числа в некотором диапазоне было получено 20 бит информации. Сколько чисел содержал этот диапазон?
7. В учениях принимает участие личный состав трех подразделений: Вымпел, СОБР и ОМОН. Причем сотрудников СОБР в 5 раза больше сотрудников Вымпел, а сотрудников ОМОН на 759 больше, чем сотрудников СОБР. Сообщение о том, что выбран сотрудник СОБР, содержало 4 бита информации. Сколько сотрудников ОМОН принимало участие в учениях?

ТЕМА №2. Методы и средства защиты информации

Практическое занятие №1

1. Стоимость защищаемой информации оценивается в 224630 единиц. Найти значение показателя риска для этой информационной системы, если вероятность взлома информационной системы, в которой эта информация размещена, равна 0.168.
2. Стоимость информационных ресурсов в некоторой информационной системе оценивается в 4284 единиц. Оценить интенсивность потока взломов информационной системы, если значение показателя риска для этой информационной системы равно 1447992 единиц.

3. Спрогнозировать вероятность взлома информационной системы №4, если интенсивность несанкционированных попыток доступа к ресурсам информационных систем №1-№4 в предшествующий прогнозу период времени была равна:

Информационная система	ИС №1	ИС №2	ИС №3	ИС №4
Количество несанкционированных попыток доступа	193	67	130	172

4. Значение показателя риска в незащищенной информационной системе равно 4509 ед. Найти значение коэффициента защищенности информационной системы, если после установки антивирусного программного обеспечения значение показателя риска стало равно 588 ед.

5. Найти значение коэффициента защищенности информационной системы, если вероятность несанкционированного доступа к ресурсам информационной системы в отсутствие средств защиты в 6 раз(а) выше вероятности несанкционированного доступа в случае наличия защитного программного обеспечения (антивирус, файрвол, антишпион).

ТЕМА №3. Криптографические методы защиты информации

Практическое занятие №1-2

1. С помощью криптосистемы Цезаря дешифровать сообщение E, если функция шифрования $F(t) = t + 9$.

E= Э Ь Ц У Я С З И Ю Е А С Щ Ч Л Й Ц С З

2. Пусть дан открытый текст T и ключ шифрования K. С помощью криптосистемы Гронсфельда найти шифртекст E.

T= А Л Г О Р И Т М Ш И Ф Р О В А Н И Я K= 7 1 5 8

3. Пусть дан открытый текст T и секретный ключ K. Используя метод Виженера найти шифртекст E.

T= М Е Т О Д Х И Л Л А K= С К Л Ц

4. С помощью криптосистемы Вижинера и ключа шифрования K дешифровать сообщение E.

1. Протестировать антивирусное программное обеспечение с помощью тестового вируса – http://www.eicar.org/anti_virus_test_file.htm.
2. Определить дату выпуска антивирусных баз, при необходимости обновить их. Рассмотреть различные способы обновления антивирусных баз.
3. Изучить интерфейс представленного антивирусного программного обеспечения – Kaspersky Internet Security.
4. Проанализировать назначение каждого компонента входящего в состав KIS, произвести настройку каждого компонента на оптимальный уровень защиты.
5. Провести полную проверку компьютера на наличие вредоносного программного обеспечения. В случае обнаружения вредоносных программ оформить отчет, в котором описать вредоносную программу, предложить методы защиты.

Практическое занятие №2

1. Установить пароль на вход в операционную систему без привлечения дополнительных программных средств.
2. Используя криптографическую программу установленную на компьютере зашифровать файлы различными криптоалгоритмами: DES single (8 byte), DES double (8 byte), AES. Оформить отчет, в котором пояснить разницу в используемых криптоалгоритмах.
3. Создать скрытый виртуальный диск на одном из логических дисков жесткого диска компьютера.
4. С помощью менеджера паролей сгенерировать пароль.
5. Сгенерированный пароль назначить на один из текстовых документов.
6. С помощью утилиты восстановления забытых паролей проанализировать защищенный документ на предмет подбора пароля.

3.5. Методические рекомендации по изучению, закреплению и контролю усвоения нового материала

ТЕМА №1. Концепции информационной безопасности

Для усвоения нового материала необходимо изучить следующие вопросы:

1. Понятие информационной безопасности. Общая концептуальная модель защиты информации
2. Политика безопасности
3. Управление рисками
4. Аудит системы управления информационной безопасностью

Для закрепления и контроля усвоения нового материала предлагается выполнить компьютерное тестирование. Тестовая оболочка: автоматизированная контролирующая система Контроль10. Время выполнения теста: 35 минут. Количество вопросов: 40. Критерий оценки: менее 60% правильных ответов – оценка неудовлетворительно, 60-70% – оценка удовлетворительно; 71-80% – оценка хорошо; более 80% – оценка отлично. Тест ориентирован на знания основных положений концептуальной модели защиты информации, нормативной базы информационной безопасности, классификации угроз и рисков безопасности, основных аспектов законодательного, административного и технического уровней защиты информации. Особый акцент в тесте делается на правильное понимание и интерпретацию обучаемыми основных терминов в сфере информационной безопасности.

ТЕМА №2. Методы и средства защиты информации

Для усвоения нового материала необходимо изучить следующие вопросы:

1. Угрозы безопасности
2. Характеристики информации
3. Общая классификация методов и средств защиты информации
4. Методы решения задач информационной безопасности
5. Средства обеспечения информационной безопасности в Internet

Для закрепления и контроля усвоения нового материала предлагается выполнить компьютерное тестирование. Тестовая оболочка: автоматизированная контролирующая система Контроль10. Время выполнения теста: 35 минут. Количество вопросов: 40. Критерий оценки: менее 60% правильных ответов – оценка неудовлетворительно, 60-70% – оценка удовлетворительно; 71-80% – оценка хорошо; более 80% – оценка отлично. Тест ориентирован на знания основных положений концептуальной модели защиты информации, нормативной базы информационной безопасности, классификации угроз и рисков безопасности, основных аспектов законодательного, административного и технического уровней защиты информации. Особый акцент в тесте делается на правильное понимание и интерпретацию обучаемыми основных терминов в сфере информационной безопасности.

ТЕМА №3. Криптографические методы защиты информации

Для усвоения нового материала необходимо изучить следующие вопросы:

1. Понятие криптографии
2. Криптографические примитивы
3. Классификация криптоалгоритмов
4. Стандарты шифрования
5. Симметричные криптосистемы
6. Анализ стойкости криптографических примитивов

Для закрепления и контроля усвоения нового материала предлагается выполнить компьютерное тестирование. Тестовая оболочка: автоматизированная контролирующая система Контроль10. Время выполнения теста: 20 минут. Количество вопросов: 25. Критерий оценки: менее 60% правильных ответов – оценка неудовлетворительно, 60-70% – оценка удовлетворительно; 71-80% – оценка хорошо; более 80% – оценка отлично. Тест ориентирован на знания следующих основных понятий и определений: криптография, криптоанализ, криптология, криптоалгоритм, классификация криптоалгоритмов, принцип Керк-

хоффа, понятие хэш-функции, генератора случайных и псевдослучайных чисел и т.д.

ТЕМА №4. Аппаратные и программные средства защиты компьютерной информации

Для усвоения нового материала необходимо изучить следующие вопросы:

1. Защита данных
 - 1.1. Шифрование дисков
 - 1.2. Архивация с шифрованием
2. Аппаратные и программные средства защиты в реализации Microsoft
3. Комплексный подход к построению системы защиты информации
4. Навесные защиты (протекторы).

Кроме того, рекомендуется:

определить понятие источника угроз информационной безопасности. Рассмотреть три группы источников угроз: человеческий фактор, технический фактор, стихийный фактор;

проанализировать различные источники распространения угроз: глобальная сеть Интернет, корпоративная сеть Интранет, электронная почта, съемные носители (дискеты, CD/DVD-диски, флеш-карты);

рассмотреть виды угроз применительно к компьютерной информации: черви, вирусы, троянские программы, программы-рекламы, программы-шпионы, потенциально опасные приложения, программы-шутки, рутикты, хакерские атаки, фишинг, спам. Изучить статистику рассмотренных выше видов угроз.

ТЕМА №5. Безопасность компьютерных сетей

Для усвоения нового материала необходимо изучить следующие вопросы:

1. Серверы
2. Рабочие станции
3. Среда передачи информации

4. Узлы коммутации сетей
5. Технологии межсетевых экранов

Для закрепления и контроля усвоения нового материала предлагается выполнить компьютерное тестирование. Тестовая оболочка: автоматизированная контролирующая система Контроль10. Время выполнения теста: 35 минут. Количество вопросов: 40. Критерий оценки: менее 60% правильных ответов – оценка неудовлетворительно, 60-70% – оценка удовлетворительно; 71-80% – оценка хорошо; более 80% – оценка отлично. Тест ориентирован на знания основных положений безопасности компьютерных сетей: основы сетевого и межсетевого взаимодействия, сетевая политика безопасности, удаленные сетевые атаки, технологии межсетевых экранов, системы обнаружения атак и вторжений.

3.6. Методические рекомендации по постановке задания к следующему занятию, по организации самостоятельной работы учащихся

ТЕМА №1. Концепции информационной безопасности

1. Изучить нормативные документы Федеральной службы по техническому и экспертному контролю, регламентирующие отношения в сфере информационной безопасности.
2. Решить практические задания:
 - а) Информационное сообщение передается в течении 5 минут со скоростью 10 байт в секунду. Сколько символов содержало данное сообщение, если был использован алфавит из 16 символов?
 - б) Даны два текста, содержащих одинаковое количество символов. Первый текст состоит из алфавита мощностью 2 символов, а второй текст – из 64 символов. Во сколько раз информации во втором тексте больше чем в первом?

ТЕМА №2. Методы и средства защиты информации

1. Провести обзор и анализ методов и средств защиты информации в реализованных проектах.
2. Разобрать теоретический материал:

Основные модели безопасного подключения к Интернет;
Принципы функционирования межсетевых экранов;
Стек протоколов TCP/IP.

ТЕМА №3. Криптографические методы защиты информации

1. Изучить одноалфавитные системы шифрования: Аффинная криптосистема, Шифр Полибия, шифр Плэйфер.
2. Рассмотреть методы вскрытия одноалфавитных систем: частотный анализ, метод полосок.
3. Проанализировать многоалфавитные системы шифрования: шифр Вернама, шифр с автоключом.

ТЕМА №4. Аппаратные и программные средства защиты компьютерной информации

1. Архивирование с шифрованием.
2. Аппаратные и программные средства защиты информации в реализации Microsoft.
3. Использование навесных защит.
4. Проанализировать слабые стороны парольной защиты операционных систем Windows.
5. Рассмотреть возможность интеграции электронных систем защиты информации с биометрическими.
6. Изучить сегментацию рынка биометрических технологий.

ТЕМА №5. Безопасность компьютерных сетей

1. Особенности применения службы проху.
2. Основные отличия статической и динамической трансляции адресов.
3. Возможные атаки при применении динамического списка контроля доступа.
4. Технологии фильтрации межсетевых экранов применяемые на уровне ядра.

4. Методические указания по изучению дисциплины (для обучающихся)

В ходе изучения дисциплины «Информационная безопасность» рекомендуется комплексно использовать знания и навыки получаемые на лекционных и практических занятиях.

Тема 1. Концепции информационной безопасности

Концептуальная модель защиты информации. Понятие объекта защиты, угрозы конфиденциальной информации, системы защиты информации. Требования к защите информации. Виды обеспечения системы защиты информации.

Правовое обеспечение информационной безопасности: нормативные документы, положения, инструкции, руководства, требования.

Классификация угроз. Источники внешних и внутренних угроз. Действия и условия приводящие к неправомерному овладению конфиденциальной информацией. Разглашение сведений. Несанкционированный доступ к конфиденциальной информации. Утечка информации.

Обеспечение защиты информации с точки зрения риска. Анализ риска. Разработка плана защиты. Реализация плана защиты. Анализ эффективности. Построение математической модели оценки эффективности системы защиты информации. Критерии оценки защищенной системы. Общее решение задачи проектирования оптимальной системы защиты.

Тема 2. Методы и средства защиты информации

Характеристики защищаемой информации. Угрозы безопасности информации: угрозы конфиденциальности, угрозы целостности, угрозы доступности.

Общая классификация методов и средств защиты информации. Технические методы защиты. Задачи, решаемые техническими методами защиты. Методы решения этих задач. Модели разграничения доступа.

Средства обеспечения информационной безопасности при работе в глобальной сети Internet. Вредоносное программное обеспечение, спам, хакерские атаки, финансовое мошенничество (фишинг, вишинг, фарминг). Популярные средства ИТ-безопасности: антивирусное программное обеспечение, межсетевые экраны, антиспамовое программное обеспечение, защита от утечки данных, виртуальные частные сети.

Тема 3. Криптографические методы защиты информации

Основные понятия и определения криптографии. История развития криптографии: наивная криптография, формальная криптография, научная криптография, компьютерная криптография, квантовая криптография.

Понятие криптоалгоритма. Классификация криптоалгоритмов: симметричные и асимметричные, подстановочные и перестановочные, потоковые и блочные.

Симметричные криптосистемы. Общая схема симметричной криптосистемы. Американские стандарты шифрования DES, AES. Российский стандарт шифрования ГОСТ 28147-89.

Алгоритмы создания цепочек. Методы рандомизации сообщений. Генераторы случайных и псевдослучайных последовательностей. Архивирование. Алгоритмы сжатия данных. Алгоритм Хаффмана. Алгоритм Лемпеля-Зива.

Асимметричные криптоалгоритмы. Общая схема асимметричной криптосистемы. Алгоритм RSA. Технологии цифровых подписей. Хэш-функция. Механизм распространения открытых ключей.

Тема 4. Аппаратные и программные средства защиты компьютерной информации

Защита данных на электронных носителях информации. Примеры криптографических и стеганографических программ, решающих задачу защиты жесткого диска от несанкционированного доступа. Архивация с шифрованием. Использование навесных защит.

Аппаратные и программные средства защиты в реализации Microsoft. Шифрование файлов в пакете программ Microsoft Office. Особенности шифрования файлов в ОС Windows. Документы PDF. Механизмы построения парольной защиты. Угрозы преодоления и способы усиления парольной защиты.

Комплексный подход к построению системы защиты информации. Биометрические технологии.

Тема 5. Безопасность компьютерных сетей

Сетевая безопасность. Классификация сетевых атак: серверы, рабочие станции, среда передачи информации, узлы коммутации сетей.

Основные защитные механизмы, меры и средства обеспечения информационной безопасности сетей. Уровни информационной инфраструктуры. Понятие межсетевых экранов. Защитные механизмы, реализуемые межсетевыми экранами. Типы межсетевых экранов. Фильтрация пакетов. Параметры фильтрации. Правила фильтрации. Реализация пакетных фильтров. Интеграция межсетевых экранов с другими средствами защиты.

ПРИЛОЖЕНИЯ

Приложение 1. Структурно-логическая схема изучения дисциплины

Темы изучаемой дисциплины	Название дисциплин и номера тем, знания по которым необходимы для оптимального изучения данной темы
Тема №1. «Концепции информационной безопасности»	Информатика и математика Тема № 17
Тема №2 «Методы и средства защиты информации»	Информационная безопасность Тема № 1
Тема №3 «Криптографические методы защиты информации»	Информационная безопасность Тема № 1, Тема № 2
Тема №4 «Аппаратные и программные средства защиты компьютерной информации»	Информационная безопасность Тема № 1- № 3
Тема №5 «Безопасность компьютерных сетей»	Информационная безопасность Тема № 1- № 4

Приложение 2. Перечень примерных вопросов (заданий) для самостоятельной работы обучающихся

1. Необходимость обеспечения безопасности в информационных системах.
2. Прогресс информационных технологий и информационная безопасность.
3. Нормативно-правовые аспекты информационной безопасности.
4. Классификация угроз безопасности информационных объектов.
5. Основные виды каналов утечки информации.
6. Умышленные и неумышленные угрозы информационной безопасности.
7. Внешние угрозы информационной безопасности.
8. Мотивы и цели компьютерных преступлений.
9. Статьи уголовного кодекса о компьютерных преступлениях.
10. Криминологическая характеристика преступлений в сфере компьютерной информации и их предупреждение.
11. Объекты информационной безопасности на предприятии.
12. Организационные методы обеспечения информационной безопасности.
13. Физическая защита информационных систем.
14. Программно - технические методы обеспечения информационной безопасности.
15. Идентификация и аутентификация.
16. Доктрина информационной безопасности Российской Федерации.
17. Государственное регулирование информационной безопасности в России.
18. Несанкционированный доступ и защита от него.
19. Проблема информационной безопасности в историческом аспекте.
20. Предупреждение компьютерных преступлений.
21. Типы компьютерных вирусов и защита от них.
22. Человеческие факторы, обуславливающие информационные угрозы.
23. Способы воздействия угроз на информационный объект.
24. Признаки воздействия вирусов на компьютерную систему.
25. Фрагментарный и системный подходы к защите информации.
26. Уголовно-правовая характеристика компьютерных преступлений.

27. Субъективная сторона компьютерных преступлений.
28. Объективная сторона компьютерных преступлений.
29. Причины и условия, способствующие совершению компьютерных преступлений.
30. Меры предупреждения преступлений в сфере компьютерной информации.
31. История вредоносных программ.
32. Исторические аспекты компьютерных преступлений.
33. Перечень сведений, которые не могут составлять коммерческую тайну.
34. Причины разглашения конфиденциальной информации.
35. Разглашение и утечка информации.
36. Стратегия злоумышленника при несанкционированном доступе.
37. Понятия информационных угроз и их виды.
38. Принципы построения системы информационной безопасности.
39. Подходы, принципы, методы и средства обеспечения безопасности.
40. Организационно-техническое обеспечение компьютерной безопасности.
41. Электронная цифровая подпись и особенности ее применения.
42. Защита информации в Интернете.
43. Этапы построения системы защиты информации.
44. Политика безопасности.
45. Оценка эффективности инвестиций в информационную безопасность.
46. Сущность криптографических методов.
47. Организационно-административные мероприятия обеспечения компьютерной безопасности.
48. Организация конфиденциального делопроизводства.
49. Принципы обеспечения информационной безопасности на основе инженерно-технического обеспечения.
50. Типы и субъекты информационных угроз.

Приложение 3. Примерный перечень вопросов (заданий) для проведения рубежного контроля.

1. Концепция и структура информационной безопасности.
2. Безопасность информации. Цель обеспечения защиты информации.
3. Система защиты информации.
4. Обеспечение защиты информации с точки зрения риска.
5. Критерии оценки защищенной системы. Общее решение задачи проектирования оптимальной системы защиты.
6. Нормативно-правовая база функционирования систем защиты информации.
7. Доктрина информационной безопасности РФ.
8. Уголовный кодекс РФ о преступлениях в сфере компьютерной безопасности.
9. Основные положения закона РФ “Об информации, информационных технологиях и о защите информации”.
10. Понятие угрозы. Классификация угроз.
11. Утечка, разглашение и несанкционированный доступ к конфиденциальной информации.
12. Характеристики информации.
13. Угрозы безопасности информации.
14. Классификация методов и средств защиты информации.
15. Технические методы защиты.
16. Задачи, решаемые техническими методами защиты. Методы решения данных задач.
17. Средства обеспечения информационной безопасности в Internet.
18. История развития, структура и основные понятия криптологии.
19. Криптография как основа информационной безопасности.
20. Подстановочные и перестановочные криптоалгоритмы.
21. Поточковые и блочные криптоалгоритмы.
22. Симметричные и асимметричные криптоалгоритмы.
23. Симметричные криптосистемы. Общая схема симметричной криптосистемы.

24. Модель криптосистемы с открытым ключом. Сертификация открытых ключей.
25. Алгоритм с открытым ключом RSA.
26. Электронная цифровая подпись. Применение хэш-функции.
27. Стандарты шифрования DES и AES.
28. Российский стандарт шифрования ГОСТ 28147-89.

Приложение 4. Примерный перечень вопросов для проведения промежуточной аттестации с рекомендациями по подготовке к зачету

29. Концепция и структура информационной безопасности.
30. Безопасность информации. Цель обеспечения защиты информации.
31. Система защиты информации.
32. Обеспечение защиты информации с точки зрения риска.
33. Критерии оценки защищенной системы. Общее решение задачи проектирования оптимальной системы защиты.
34. Нормативно-правовая база функционирования систем защиты информации.
35. Доктрина информационной безопасности РФ.
36. Уголовный кодекс РФ о преступлениях в сфере компьютерной безопасности.
37. Основные положения закона РФ “Об информации, информационных технологиях и о защите информации”.
38. Понятие угрозы. Классификация угроз.
39. Утечка, разглашение и несанкционированный доступ к конфиденциальной информации.
40. Характеристики информации.
41. Угрозы безопасности информации.
42. Классификация методов и средств защиты информации.
43. Технические методы защиты.
44. Задачи, решаемые техническими методами защиты. Методы решения данных задач.
45. Средства обеспечения информационной безопасности в Internet.
46. История развития, структура и основные понятия криптологии.
47. Криптография как основа информационной безопасности.
48. Подстановочные и перестановочные криптоалгоритмы.
49. Поточковые и блочные криптоалгоритмы.
50. Симметричные и асимметричные криптоалгоритмы.

51. Симметричные криптосистемы. Общая схема симметричной криптосистемы.
52. Модель криптосистемы с открытым ключом. Сертификация открытых ключей.
53. Алгоритм с открытым ключом RSA.
54. Электронная цифровая подпись. Применение хэш-функции.
55. Стандарты шифрования DES и AES.
56. Российский стандарт шифрования ГОСТ 28147-89.
57. Защита информации на электронных носителях информации.
58. Архивация с шифрованием.
59. Аппаратные и программные средства защиты в реализации Microsoft.
60. Принципы построения парольной защиты.
61. Традиционные средства защиты компьютерной информации и их недостатки.
62. Комплексный подход к построению систем безопасности.
63. Классификация сетевых атак по цели.
64. Меры и средства обеспечения информационной безопасности компьютерных сетей.
65. Задачи защиты информации в компьютерных сетях и методы их решения.
66. Понятие межсетевых экранов. Типы межсетевых экранов.
67. Защитные механизмы, реализуемые межсетевыми экранами.
68. Интеграция межсетевых экранов с другими средствами защиты.

Приложение 5. Учебно-методическое обеспечение дисциплины

Основная литература:

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ. // Собрание законодательства РФ. 2006. № 31. Ст. 3448.
2. Федеральный закон «Об электронной цифровой подписи» от 10.01.2002 № 1-ФЗ. // Собрание законодательства РФ. 2002. № 2. Ст. 127.
3. Закон РФ «О безопасности» от 05.03.1992 № 2446-1 (ред. от 02.03.2007) // Ведомости Верховного Совета РФ . 1992. № 15. Ст. 769.
4. Закон РФ «О правовой охране программ для электронно-вычислительных машин и баз данных» от 23.09.1992 № 3523-1 (ред. от 02.02.2006) // Ведомости Верховного Совета РФ . 1992. № 42. Ст. 2325.
5. Доктрина информационной безопасности РФ. Совм. Изд. Ред. «Российская газета» и Международной академии информатизации. – М.: Информациология, 2000.
6. Михайленко Е.В. Информационная безопасность: курс лекций / И.Н. Старостенко. – Краснодар: Краснодарская академия МВД России, 2005.
7. Ярочкин В.И. Информационная безопасность: учебник. – М.: Фонд «Мир», 2003.

Дополнительная литература:

Тема 1. Концепции информационной безопасности

1. Мельников В.П. Информационная безопасность и защита информации: учебное пособие / С.А. Клейменов. – М.: Академия, 2008.

Тема 2. Методы и средства защиты информации

2. Старостенко И.Н. Методы защиты компьютерной информации: лекция. – Краснодар: Краснодарский университет МВД России, 2006.

Тема 3. Криптографические методы защиты информации

3. Старостенко И.Н. Криптографические средства защиты информации: лекция. – Краснодар: Краснодарский университет МВД России, 2006.

Тема 4. Аппаратные и программные средства защиты компьютерной ин-

формации

4. Скляр Д.В. Искусство защиты и взлома информации. – СПб.: БХВ Петербург, 2005.

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

Тема 5. Безопасность компьютерных сетей

6. Галицкий А.В. Защита информации в сети – анализ технологий и синтез решений - М.: ДМК Пресс, 2004.

Приложение 6. Перечень мультимедийного сопровождения лекционных занятий

1. Мультимедийная презентация «Концепции информационной безопасности».
2. Мультимедийная презентация «Методы и средства защиты информации».
3. Мультимедийная презентация «Криптографические методы защиты информации».
4. Мультимедийная презентация «Аппаратные и программные средства защиты информации».
5. Мультимедийная презентация «Безопасность компьютерных сетей».

Приложение 7. Перечень компьютерных обучающих программ

1. Компьютерная обучающая программа «Концепции информационной безопасности».
2. Компьютерная обучающая программа «Оценка рисков».
3. Компьютерная обучающая программа «Элементы криптографии».