В. П. Рядченко
А. Х. Башиева
Л. К. Бостанова

КОМПЛЕКСНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебно-методическое пособие для магистрантов 1 курса направления подготовки 09.04.03 Прикладная информатика

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ ГУМАНИТАРНО-ТЕХНОЛОГИЧЕСКАЯ АКАДЕМИЯ

В. П. Рядченко
А. Х. Башиева
Л. К. Бостанова

КОМПЛЕКСНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебно-методическое пособие для магистрантов 1 курса направления подготовки 09.04.03 Прикладная информатика

Черкесск
2016

УДК 004.05
ББК 32.97
Р-75

Рассмотрено на заседании кафедры «Информатика и информационные технологии»
Протокол № 6 от « 22» декабря 2015 г.
Рекомендовано к изданию редакционно-издательским советом СевКавГГТА.
Протокол № от « 12 » января 2016 г.

Рецензент: Эркенов С.Б. – и.о. директора РГБУ «Уполномоченный многофункциональный центр представления гос. и муниц. услуг -Центр информационных технологий КЧР»

Р-75 Рядченко В. П. Комплексная информационная безопасность: учебно-методическое пособие для магистрантов 1 курса направления подготовки 09.04.03 Прикладная информатика/В.П. Рядченко, А. Х. Башиева, Л. К. Бостанова – Черкесск: БИЦ СевКавГГТА, 2016. – 40 с.

Учебно-методическое пособие содержит практические и тестовые задания, тематику устных работ, методические рекомендации и др. для самостоятельной подготовки магистрантов к прохождению текущей и промежуточной аттестации по дисциплине «Комплексная информационная безопасность».

УДК 004.05
ББК 32.97

Содержание

Введение

Современный специалист в области информационных технологий должен обладать знаниями и навыками обеспечения информационной безопасности. Связано это с тем, что в информационных системах предприятий и организаций хранится и обрабатывается критически важная информация, нарушение конфиденциальности, целостности или доступности, которой может привести к нежелательным последствиям. Поэтому вопросам обеспечения информационной безопасности должно уделяться внимание на всех этапах разработки и эксплуатации информационных систем.

В данном пособии изложен материал учебной дисциплины «Комплексная информационная безопасность», в ходе изучения которой, студенты получают базовые знания о теории защиты информации, методах и средствах обеспечения информационной безопасности, а также практические навыки организации защиты информационных систем.

В учебно-методических указаниях приводятся рекомендации по всем формам работы магистрантов: по теоретическому курсу, по практическим занятиям, по самостоятельной работе. Также приводятся требования к прохождению текущей и промежуточной аттестации по дисциплине.

1. Цели и задачи изучения дисциплины

Цель освоения дисциплины «Комплексная информационная безопасность» состоит в изучении различных методов и средств по построению комплексной системы информационной безопасности современной организации.

Задачи изучения дисциплины – знание основных аспектов комплексной информационной безопасности, в том числе технических средств защиты информации, обеспечения безопасности сетевых коммуникаций, основ криптографии и криптоанализа, основных методов, законов и нормативных актов обеспечения информационной безопасности.

Дисциплина «Комплексная информационная безопасность» относится к вариативной части обязательных дисциплин Блока 1 Дисциплины (модули) (Б1.В.ОД.3), имеет тесную связь с другими дисциплинами.

Планируемые результаты освоения образовательной программы (ОП) – компетенции обучающихся определяются требованиями стандарта по направлению подготовки и формируются в соответствии с матрицей компетенций ОП

№ п/п	Номер/ индекс компетенции	Наименование компетенции (или ее части)	В результате изучения дисциплины обучающиеся должны:
1	2	3	4
1.	ОК-2	готовностью действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения	**Знать:** варианты поведения в нестандартных ситуациях **Уметь:** действовать в нестандартных ситуациях и нести социальную и этическую ответственность за принятые решения **Владеть:** навыками действовать в нестандартных ситуациях и нести социально-этическую ответственность за принятые решения
2.	ПК-14	способностью принимать эффективные проектные решения в условиях неопределенности и риска	**Знать:** методы и нотации описания бизнес-процессов, типологию информационных сервисов **Уметь:** разрабатывать регламенты исполнения бизнес-процессов **Владеть:** навыками подготовки технико-экономического обоснования; навыками работы с CASE-системами
3.	ПК-15	способностью формировать стратегию информатизации прикладных процессов и создания прикладных ИС в соответствии со стратегией развития предприятий	**Знать:** об основных методологиях и технологиях реинжиниринга и последующего управления бизнес-процессами **Уметь:** адаптировать приложения к изменяющимся условиям функционирования **Владеть:** методами оценки и выбора информационно-коммуникационных технологий

В результате изучения дисциплины магистрант должен усвоить:

- принципы организации комплексной информационной безопасности, применяемые при построении защищенной информационной системы предприятия;
- стандарты обеспечения информационной безопасности;
- методы организации защиты данных, а так же прикладного и системного программного обеспечения;
- методики организации поддержки пользователей, выполняющих прием, обработку, передачу и хранение данных ограниченного доступа на ПЭВМ;
- функциональные возможности систем, и программно-технических комплексов, обеспечивающих защиту информации;
- функции и основные обязанности подразделения, обеспечивающего информационную безопасность предприятия.

Магистрант должен научиться:

- анализировать архитектуру информационных систем в целях организации защиты обрабатываемой информации;
- использовать программно-технические средства для защиты обрабатываемой информации.

2. Лекции

Лекция является основной формой обучения в высшем учебном заведении. Записи лекций в конспектах должны быть избирательными, полностью следует записывать только определения. В конспекте рекомендуется применять сокращение слов, что ускоряет запись. Вопросы, возникающие в ходе лекции, рекомендуется записывать на полях и после окончания лекции обратиться за разъяснением к преподавателю. Необходимо активно работать с конспектом лекции: после окончания лекции рекомендуется перечитать свои записи, внести поправки и дополнения на полях.

Работа над конспектом лекции осуществляется по этапам:

- повторить изученный материал по конспекту;
- непонятные положения отметить на полях и уточнить;
- неоконченные фразы, пропущенные слова и другие недочеты в записях устранить, пользуясь материалами из учебника и других источников;
- завершить техническое оформление конспекта (подчеркивания, выделение главного, выделение разделов, подразделов и т.п.).

Содержание лекций

Тема 1. Основные понятия безопасности информационных технологий. Изучение федеральных законов в области информационной безопасности.

Актуальность проблемы обеспечения информационной безопасности. Термины и определения в области информационной безопасности. Правовое регулирование применения СКЗИ и ЭП в корпоративных информационных системах. Специальные нормативные и методические документы ФСБ России по использованию шифровальных(криптографических) средств. Изучение федеральных законов в области информационной безопасности: «Об электронной подписи» 2011 года, «О персональных данных», «Об информации, информационных технологиях и защите информации» 2006 года с дополнениями 2014 года.

Основная литература:

1. Артемов, А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.– Электрон. текстовые данные.– Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.– 256 с.– Режим доступа: http://www.iprbookshop.ru/33430.– ЭБС «IPRbooks», по паролю

2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.– Электрон. текстовые данные.– Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.– 113 с.– Режим доступа: http://www.iprbookshop.ru/43183.– ЭБС «IPRbooks», по паролю

Дополнительная литература:

1. Петров, С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.– Электрон. текстовые данные.– Саратов: Ай Пи Ар Букс, 2015.– 326 с.– Режим доступа: http://www.iprbookshop.ru/33857.– ЭБС «IPRbooks», по паролю

Тема 2. Защита от несанкционированного доступа к информации. Конфиденциальная информация, конфиденциальный документооборот.

Защита от несанкционированного доступа к информации. Организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа. Конфиденциальная информация. Изучение понятий государственная тайна, коммерческая тайна, персональные данные, данные ограниченного доступа. Правовые документы в области защиты конфиденциальных сведений.

Основная литература:

1. Артемов, А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.– Электрон. текстовые данные.– Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.– 256 с.– Режим доступа: http://www.iprbookshop.ru/33430.– ЭБС «IPRbooks», по паролю

2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.– Электрон. текстовые данные.– Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.– 113 с.– Режим доступа: http://www.iprbookshop.ru/43183.– ЭБС «IPRbooks», по паролю

Дополнительная литература:

1. Петров, С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.– Электрон. текстовые данные.– Саратов: Ай Пи Ар Букс, 2015.– 326 с.– Режим доступа: http://www.iprbookshop.ru/33857.– ЭБС «IPRbooks», по паролю

Тема 3. Построение модели угроз и модели нарушителей информационной безопасности.

Модель угроз и модель нарушителей информационной безопасности. Схема построения моделей на основе стандартов ИБ.

Основная литература:

1. Артемов, А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.– Электрон. текстовые данные.– Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.– 256 с.– Режим доступа: http://www.iprbookshop.ru/33430.– ЭБС «IPRbooks», по паролю

2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.– Электрон. текстовые

данные.– Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.– 113 с.– Режим доступа: http://www.iprbookshop.ru/43183.– ЭБС «IPRbooks», по паролю

Дополнительная литература:

1. Петров, С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.– Электрон. текстовые данные.– Саратов: Ай Пи Ар Букс, 2015.– 326 с.– Режим доступа: http://www.iprbookshop.ru/33857.– ЭБС «IPRbooks», по паролю

Тема 4. Основные понятия аудита и оценки возможных рисков информационной безопасности.

Аудит и оценка возможных рисков ИБ. Основные понятия.

Основная литература:

1. Артемов, А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.– Электрон. текстовые данные.– Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.– 256 с.– Режим доступа: http://www.iprbookshop.ru/33430.– ЭБС «IPRbooks», по паролю
2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.– Электрон. текстовые данные.– Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.– 113 с.– Режим доступа: http://www.iprbookshop.ru/43183.– ЭБС «IPRbooks», по паролю

Дополнительная литература:

1. Петров, С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.– Электрон. текстовые данные.– Саратов: Ай Пи Ар Букс, 2015.– 326 с.– Режим доступа: http://www.iprbookshop.ru/33857.– ЭБС «IPRbooks», по паролю

Тема 5. Основные типы атак на информационные системы, основные меры противодействия. Компьютерные вирусы и защита от них.

Основные типы атак на информационные системы и меры их защиты. Протокол IPsec. Методы аутентификации и шифрования протокола IPsec.

Основная литература:

1. Артемов, А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.– Электрон. текстовые данные.– Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.– 256 с.– Режим доступа: http://www.iprbookshop.ru/33430.– ЭБС «IPRbooks», по паролю
2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.– Электрон. текстовые данные.– Самара: Самарский государственный архитектурно-строительный

университет, ЭБС АСВ, 2014.– 113 с.– Режим доступа: http://www.iprbookshop.ru/43183.– ЭБС «IPRbooks», по паролю

Дополнительная литература:

1. Петров, С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.– Электрон. текстовые данные.– Саратов: Ай Пи Ар Букс, 2015.– 326 с.– Режим доступа: http://www.iprbookshop.ru/33857.– ЭБС «IPRbooks», по паролю

3. Практические занятия

При подготовке к практическим занятиям следует использовать основную литературу из представленного списка рабочей программе, а также руководствоваться приведенными указаниями.

Магистранту рекомендуется следующая схема подготовки к семинарскому занятию:

- проработать конспект лекций;
- проанализировать основную и дополнительную литературу, рекомендованную по изучаемому разделу;
- при затруднениях сформулировать вопросы к преподавателю.

Содержание практических занятий.

Практическое занятие № 1

Тема 1. Безопасность информационных технологий.

Цель занятия: Построение системы безопасности предприятия. Разбор основных понятий ФЗ «Об электронной подписи».

Вопросы для обсуждения:

1. Основные требования к системам обеспечения комплексной защиты информации.
2. Основные положения ФЗ: 1. Об электронной подписи 2011 2. Об информации, информационных технологиях и защите информации, 2006 (с поправками 2014 года)

Основная литература:

1. Артемов, А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.– Электрон. текстовые данные.– Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.– 256 с.– Режим доступа: http://www.iprbookshop.ru/33430.– ЭБС «IPRbooks», по паролю

2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.– Электрон. текстовые данные.– Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.– 113 с.– Режим доступа: http://www.iprbookshop.ru/43183.– ЭБС «IPRbooks», по паролю

Дополнительная литература:

1. Петров, С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.– Электрон. текстовые данные.– Саратов: Ай Пи Ар Букс, 2015.– 326 с.– Режим доступа: http://www.iprbookshop.ru/33857.– ЭБС «IPRbooks», по паролю

Практическое занятие № 2

Тема 2. Конфиденциальная информация. Несанкционированный доступ к информации.

Цель занятия: Разбор методов и средств защиты от несанкционированного доступа к информации. Разбор понятий конфиденциального документооборота.

Вопросы для обсуждения:

1. Методы защиты информации при передаче по сетям.
2. Методы и средства защиты от несанкционированного доступа к информации.
3. Понятия конфиденциального документооборота.

Основная литература:

1. Артемов, А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.– Электрон. текстовые данные.– Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.– 256 с.– Режим доступа: http://www.iprbookshop.ru/33430.– ЭБС «IPRbooks», по паролю

2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.– Электрон. текстовые данные.– Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.– 113 с.– Режим доступа: http://www.iprbookshop.ru/43183.– ЭБС «IPRbooks», по паролю

Дополнительная литература:

1. Петров, С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.– Электрон. текстовые данные.– Саратов: Ай Пи Ар Букс, 2015.– 326 с.– Режим доступа: http://www.iprbookshop.ru/33857.– ЭБС «IPRbooks», по паролю

Практическое занятие № 3

Тема 3. Модель угроз и модель нарушителей информационной безопасности.

Цель занятия: Построение модели угроз и нарушителей информационной безопасности на примере.

Вопросы для обсуждения:

1. Построение модели угроз для информационной системы предприятия.
2. Модели угроз и нарушителей информационной безопасности на примере.

Основная литература:

1. Артемов, А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.– Электрон. текстовые данные.– Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.– 256 с.– Режим доступа: http://www.iprbookshop.ru/33430.– ЭБС «IPRbooks», по паролю

2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.– Электрон. текстовые данные.– Самара: Самарский государственный архитектурно-строительный

университет, ЭБС АСВ, 2014.– 113 с.– Режим доступа: http://www.iprbookshop.ru/43183.– ЭБС «IPRbooks», по паролю

Дополнительная литература:

1. Петров, С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.– Электрон. текстовые данные.– Саратов: Ай Пи Ар Букс, 2015.– 326 с.– Режим доступа: http://www.iprbookshop.ru/33857.– ЭБС «IPRbooks», по паролю

Практическое занятие № 4

Тема 4. Аудит и оценка возможных рисков ИБ.

Цель занятия Аудит и оценка возможных рисков ИБ предприятия на примере.

Вопросы для обсуждения:

1. Аудит и оценка возможных рисков ИБ предприятия.
2. Построить таблицу рисков угроз ИБ для конкретной ИС.

Основная литература:

1. Артемов, А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.– Электрон. текстовые данные.– Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.– 256 с.– Режим доступа: http://www.iprbookshop.ru/33430.– ЭБС «IPRbooks», по паролю
2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.– Электрон. текстовые данные.– Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.– 113 с.– Режим доступа: http://www.iprbookshop.ru/43183.– ЭБС «IPRbooks», по паролю

Дополнительная литература:

1. Петров, С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.– Электрон. текстовые данные.– Саратов: Ай Пи Ар Букс, 2015.– 326 с.– Режим доступа: http://www.iprbookshop.ru/33857.– ЭБС «IPRbooks», по паролю

Практическое занятие № 5

Тема 5. Основные типы атак на информационные системы, основные меры противодействия. Компьютерные вирусы и защита от них.

Цель занятия: Изучение протокола IPsec. Разбор на примерах.

Вопросы для обсуждения:

1. Основные типы атак на информационные системы.
2. Основные меры противодействия.
3. Компьютерные вирусы и защита от них.
4. Анализ системы внешних и внутренних угроз информационной системе предприятия.
5. Построить модель нарушителя для информационной системы вуза.

Основная литература:

1. Артемов, А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.– Электрон. текстовые данные.– Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.– 256 с.– Режим доступа: http://www.iprbookshop.ru/33430.– ЭБС «IPRbooks», по паролю

2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.– Электрон. текстовые данные.– Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.– 113 с.– Режим доступа: http://www.iprbookshop.ru/43183.– ЭБС «IPRbooks», по паролю

Дополнительная литература:

1. Петров, С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.– Электрон. текстовые данные.– Саратов: Ай Пи Ар Букс, 2015.– 326 с.– Режим доступа: http://www.iprbookshop.ru/33857.– ЭБС «IPRbooks», по паролю

4. Самостоятельная работа

Самостоятельная работа студентов в рамках изучения дисциплины «Комплексная информационная безопасности» регламентируется общим графиком учебной работы, предусматривающим посещение семинарских занятий, выполнение заданий. При организации самостоятельной работы по дисциплине «Комплексная информационная безопасности» студенту следует:

1. Внимательно изучить материалы, характеризующие курс и тематику самостоятельного изучения, что изложено в учебно-методическом комплексе по дисциплине. Это позволит четко представить, как круг изучаемых тем, так и глубину их постижения.

2. Составить подборку литературы, достаточную для изучения предлагаемых тем. В программе дисциплины представлены основной и дополнительный списки литературы. Они носят рекомендательный характер, это означает, что всегда есть литература, которая может не входить в данный список, но является необходимой для освоения темы. При этом следует иметь в виду, что нужна литература различных видов: учебники, учебные и учебно-методические пособия; первоисточники, монографии, сборники научных статей, публикации в журналах, любой эмпирический материал; справочная литература – энциклопедии, словари, тематические, терминологические справочники, раскрывающие категориально- понятийный аппарат.

3. Основное содержание той или иной проблемы следует уяснить, изучая учебную литературу.

4. Абсолютное большинство проблем носит не только теоретический, умозрительный характер, но самым непосредственным образом выходят на жизнь, они тесно связаны с практикой социального развития, преодоления противоречий и сложностей в обществе. Это предполагает наличие у студентов не только знания категорий и понятий, но и умения использовать их в качестве инструмента для анализа социальных проблем. Иными словами, студент должен совершать собственные, интеллектуальные усилия, а не только механически заучивать понятия и положения.

5. Соотнесение изученных закономерностей с жизнью, умение достигать аналитического знания предполагает у студента мировоззренческой культуры. Формулирование выводов осуществляется, прежде всего, в процессе творческой дискуссии, протекающей с соблюдением методологических требований к научному познанию.

Основными видами самостоятельной работы по курсу «Комплексная информационная безопасности» являются:

- изучение теоретических вопросов при подготовке к семинарам, подготовке к тестовому контролю, к внеаудиторной контактной работе;
- осмысление информации, сообщаемой преподавателем, ее обобщение и краткая запись;
- своевременная доработка конспектов лекций;

- подбор, изучение, анализ и конспектирование рекомендуемой литературы;
- подготовка к экзамену.

Вопросы для самостоятельного изучения по дисциплине «Комплексная информационная безопасность»

1. Понятия безопасности информационных технологий.
2. Нормативная база обеспечения информационной безопасности.
3. Защита от несанкционированного доступа к информации.
4. Модель угроз и модель нарушителей информационной безопасности.
5. Аудит и оценка возможных рисков ИБ.
6. Основные типы атак на информационные системы, основные меры противодействия.

5. Фонд оценочных средств для проведения текущего контроля

Список вопросов для проведения текущего контроля и устного опроса обучающихся:

1. Требования руководящих документов по порядку разработки и содержанию «Положения о подразделении (специалисте) по защите информации».
2. Организационные мероприятия, проводимые с целью защиты СВТ и АС от НСД.
3. Четыре основные составляющие национальных интересов РФ в информационной сфере.
4. Требования руководящих документов по порядку разработки и содержанию «Руководства по защите информации …».
5. Внешние источники угроз безопасности информации.
6. Типовой перечень внутренних организационно-распорядительных документов по защите конфиденциальной информации.
7. Внутренние источники угроз безопасности информации.
8. Основные направления обеспечения защиты информации от НСД.
9. Положение по аттестации объектов информатизации.
10. Основные принципы защиты информации от НСД.
11. Порядок согласования и утверждения Руководства по защите информации.
12. Что такое информационная безопасность?
13. В чем заключаются интересы личности в информационной сфере?
14. В чем заключаются интересы общества в информационной сфере?
15. В чем заключаются интересы государства в информационной сфере?
16. Четыре основные составляющие национальных интересов РФ?
17. Виды угроз?
18. Внешние источники угроз?
19. Внутренние источники угроз?

Критерии оценки:

Оценка «отлично» выставляется обучающемуся, если он свободно владеет терминологией, демонстрирует прекрасное знание предмета, соединяя при ответе знания из разных разделов дисциплины, добавляя комментарии, пояснения, может быстро и безошибочно проиллюстрировать ответ собственными примерами. Владеет аргументацией, грамотной, доступной и понятной речью.

Оценка «хорошо», владеет терминологией, делая ошибки, при неверном употреблении сам может их исправить, хорошо владеет содержанием изучаемой темы, видит взаимосвязи, может провести анализ, но не всегда делает это самостоятельно без помощи преподавателя, может подобрать соответствующие примеры, чаще из имеющихся в учебных материалах. Хорошая аргументация, четкость, лаконичность ответов.

Оценка «удовлетворительно», редко использует при ответе термины, подменяет одни понятия другими, не всегда понимая разницы, отвечает на конкретный вопрос соединяя знания только при наводящих вопросах преподавателя, с трудом может соотнести теорию и практические примеры из учебных материалов; примеры не всегда правильные. Слабая аргументация, нарушена логика при ответе, однообразные формы изложения мыслей.

Оценка «неудовлетворительно», при ответе не владеет профессиональной терминологией. Неуверенное и логически непоследовательно излагает материал, обнаруживает пробелы в знаниях основного учебного материала, не может привести примеры из учебной литературы, затрудняется с ответом на поставленные преподавателем вопросы.

Тестовые задания для входного контроля по дисциплине «Комплексная информационная безопасность»

Цель входного контроля – определить начальный уровень подготовленности обучающихся и выстроить индивидуальную траекторию обучения. В условиях личностно-ориентированной образовательной среды результаты входного оценивания студента используются как начальные значения в индивидуальном профиле академической успешности студента.

1. За единицу количества информации принимается:
a) Байт;
b) Код;
c) Бит;
d) Бод;
2. В какой из последовательностей единицы измерения указаны в порядке возрастания:
a) гигабайт, мегабайт, килобайт, байт;
b) мегабайт, килобайт, байт, гигабайт;
c) гигабайт, килобайт, мегабайт, байт;
d) байт, килобайт, мегабайт, гигабайт;
3. Свойство информации, определяющее ее достаточность для принятия решения называется:
a) Достоверность;
b) Адекватность;
c) Полнота;
d) Доступность;
4. Сколько бит в сообщении объемом четверть килобайта?
a) 250;
b) 512;
c) 2000;
d) 2048;

5. Комплекс аппаратных и программных средств, позволяющих компьютерам обмениваться данными, – это:
a) Магистраль;
b) Шина данных;
c) Компьютерная сеть;
d) Интерфейс;
6. Глобальная компьютерная сеть – это;
a) множество компьютеров, связанных каналами передачи информации и находящихся в пределах одного помещения, здания;
b) совокупность хост - компьютеров и файл-серверов;
c) совокупность локальных сетей и компьютеров, расположенных на больших расстояниях и соединенных с помощью каналов связи в единую систему;
d) информационная система с гиперсвязями;
7. Аппаратное подключение периферийного устройства к магистрали производится через:
a) Регистр;
b) Драйвер;
c) Контроллер;
d) Стример;
8. Что такое Кэш-память?
a) память, предназначенная для долговременного хранения информации, независимо от того, работает ЭВМ или нет;
b) это сверхоперативная память, в которой хранятся наиболее часто используемые участки оперативной памяти;
c) память, в которой хранятся системные файлы операционной системы;
d) память, в которой обрабатывается одна программа в данный момент времени;
9. При выключении компьютера вся информация стирается:
a) на гибком диске;
b) на CD-диске;
c) на жестком диске;
d) в оперативной памяти;
10. Устройством ввода является...
a) Сканер;
b) Принтер;
c) Стример;
d) Дисплей;
11. Что является характеристикой монитора? ...
a) цветовое разрешение;
b) тактовая частота;
c) дискретность;
d) время доступа к информации;
12. К прикладному программному обеспечению не относятся:
a) текстовые процессоры;

b) СУБД;
c) Операционные оболочки;
d) Игры;

13. Минимальным объектом, используемым в растровом графическом редакторе, является...

a) точка экрана (пиксель);
b) объект (прямоугольник, круг и т.д.);
c) палитра цветов;
d) знакоместо (символ);

14. Минимальным объектом, используемым в векторном графическом редакторе, является...

a) точка экрана (пиксель);
b) объект (прямоугольник, круг и т.д.);
c) палитра цветов;
d) знакоместо (символ);

15. Программа Excel используется для...

a) создания текстовых документов;
b) создания электронных таблиц;
c) создания графических изображений;
d) все варианты верны;

16. Адрес диапазона ячеек в Excel задаётся указанием:

a) ссылок первой и последней его ячеек;
b) указанием имени листа;
c) указанием имени файла;
d) указанием адреса последней ячейки;

17. Свойство алгоритмов, означающие, что результат выполнения алгоритма не зависит от исполнителя, а определяется только входными данными и шагами:

a) Результативность;
b) Детерминированность;
c) Дискретность:
d) Определенность.

18. Совокупность данных, сохраняемых внутри некоторой системы, – это информация

a) Внешняя;
b) Выходная;
c) Внутренняя;
d) Промежуточная;

19. Модель системы – это:

a) описание системы, отображающее определенную группу ее свойств;
b) возникновение и сохранение структуры и целостных свойств системы;
c) множество существенных свойств, которыми система обладает в данный момент времени;
d) порядок системы;

20. Осуществляет сбор, передачу и переработку информации об объекте:

a) информационное пространство;
b) информационная система;
c) информационная среда;
d) информационный рынок;

21. Хранение и поиск информации являются фундаментальными функциями:

a) локальных баз данных;
b) корпоративных информационных систем;
c) справочной системы;
d) автоматизированных информационных систем;

22. Свойство производительности информационной системы – это:

a) время отклика на запрос клиента;
b) максимальное использование ресурсов памяти компьютеров;
c) максимальное использование возможностей аппаратного обеспечения информационной системы;
d) пропускная способность информационной системы;

23. Корпоративные информационные системы – это:

a) информационная система, осуществляющая бизнес в Интернете;
b) информационная система, предоставляющая услуги по доступу в Интернет;
c) компьютерная сеть корпорации;
d) информационная система, обеспечивающая работу корпорации;

24. Распределенные информационные системы могут быть:

a) клиент-серверными или файл-серверными;
b) корпоративными или вычислительными;
c) автоматизированными или клиент-серверными;
d) персональными или экономическими;

25. Для ввода, обработки, хранения и поиска графических образов бумажных документов, предназначены:

a) системы управления проектами;
b) системы автоматизации деловых процедур;
c) системы обработки изображений документов;
d) системы оптического распознавания символов;

26. Для управления файлами и папками в ОС Windows можно использовать;

a) программу проводник;
b) панель задач;
c) панель управления;
d) меню кнопки «Пуск»;

27. World Wide Web – это служба Интернет, предназначенная для:

a) поиска и просмотра гипертекстовых документов, включающих в себя графику, звук и видео;
b) передачи файлов;
c) передачи электронных сообщений;
d) общения в реальном времени с помощью клавиатуры;

28. COM – это:
a) программные компоненты;
b) коммерческий сервер;
c) коммутатор;
d) среда объектно-ориентированного программирования;
29. Структура системы – это:
a) совокупность элементов и связей между ними;
b) совокупность подсистем;
c) описание системы, отображающее определенную группу ее свойств;
d) порядок системы;
30. Какие функции не выполняют Информационные системы;
a) информационно-справочные;
b) Контрольные;
c) Расчетные;
d) Организационные;

Критерии оценки:

Оценивание тестирования.

- от 0 до 49,9 % выполненного решения – неудовлетворительно;
- от 50% до 69,9% – удовлетворительно;
- от 70% до 89,9% – хорошо;
- от 90% до 100% – отлично

Тестовые задания к проведению текущего контроля по дисциплине «Комплексная информационная безопасность»

Тесты к разделу 1
1. Информационная безопасность – это (ОК-2):
1)Защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации;
2) Защищенность информации от несанкционированного доступа;
3) Защищенность информации от случайных или преднамеренных воздействий естественного или искусственного характера;
4) Защищенность информации от внешнего воздействия.
2. Административный уровень включает (ОК-2):
1)Комплекс взаимокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации;
2) Комплекс мероприятий, реализующих практические механизмы уничтожения защищаемой информации с истекшим сроком хранения;

3) Комплекс мероприятий, реализующих практические механизмы эксплуатации систем защиты информации;
4) Комплекс приказов и распоряжений, устанавливающих степень ответственности работников организации при работе с защищаемой информацией.

3. Защита информации это (ОК-2):

1) Процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2) Преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3) Получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4) Совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5)Деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

4. Что из перечисленного не относится к числу основных аспектов информационной безопасности (ОК-2):

1) Доступность;
2) Целостность;
3)Защита от копирования;
4) Конфиденциальность.

5. В алгоритмах этого вида и для шифрования, и для дешифрования информации применяется один и тот же секретный ключ (ПК-15):

1) Симметричные алгоритмы;
2) Ассиметричные алгоритмы;
3) Алгоритмы Ньютона-Дирихле.

6. Нарушитель информационной безопасности – это (ОК-2):

1) Субъект (лицо или группа лиц), который предпринял попытку выполнения запрещенных операций (действий) по ошибке или незнанию;
2)Субъект (лицо или группа лиц), реализующий угрозы информационной безопасности организации (по ошибке, незнанию или осознанно), путем нарушения предоставленных ему полномочий по доступу к активам организации или по распоряжению ими;
3) Субъект (лицо или группа лиц), который предпринял попытку выполнения запрещенных операций (действий) осознанно со злым умыслом;
4) Работник организации, выполнивший запрещенную операцию путем нарушения предоставленных ему полномочий.

7. Главными составляющими информационной безопасности являются (ПК-14):

1) Целостность;
2) Доступность;
3) Конфиденциальность;
4)Все вместе взятое.

8. Целостность информации – это (ПК-14):

1)Гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений;

2) Информация не повреждена, может быть прочитана и обработана;

3) Информация была обработана без обнаружения ошибок.

9. Что такое процедура (ПК-14)?

1) Правила использования программного и аппаратного обеспечения в организации;

2)Пошаговая инструкция по выполнению задачи;

3) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах;

4) Обязательные действия персонала

10. Что такое политики безопасности (ПК-14)?

1) Пошаговые инструкции по выполнению задач безопасности;

2) Общие руководящие требования по достижению определенного уровня безопасности;

3) Широкие, высокоуровневые заявления руководства;

4) Детализированные документы по обработке инцидентов безопасности.

11. Законодательно-правовой уровень включает (ПК-14):

1)Комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус.

2) Комплекс приказов и распоряжений организации, устанавливающих правовой статус информационных отношений между работниками, методы, формы и способы защиты;

3) Комплекс законодательных и иных правовых актов органов местного самоуправления, устанавливающих правовой статус субъектов информационных отношений, объектов защиты, методы, формы и способы защиты;

12. Информация по доступу к ней бывает (ПК-15):

1) открытая (общедоступная) и закрытая (конфиденциальная);

2) избыточная, достаточная и недостаточная;

3) исходная, промежуточная и результирующая;

4) постоянная, переменная и смешанная.

Тесты к разделу 2

1. Отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (ПК-14):

1)Информационные ресурсы;

2) Реляционная база данных;

3) Файловая база данных;

4) D-дерево.

2. Защита информации – это (ОК-2):

1) Комплекс мероприятий, направленных на обеспечение информационной безопасности;
2)Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;
3) Комплекс мероприятий, направленных на предотвращение утечки информации;
4) Комплекс мероприятий, направленных на поиск нарушителя информационной безопасности.

3. Кто является основным ответственным за определение уровня классификации информации по степени важности (ПК-14)?

1) Руководитель среднего звена;
2) Руководитель организации или замещающее его лицо;
3)Владелец;
4) Пользователь.

4. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности (ПК-14)?

1) Поддержка;
2)Выполнение анализа рисков;
3) Определение цели и границ;
4) Делегирование полномочий.

5. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом (ПК-14)?

1) Безопасная OECD;
2) ISO\IEC;
3)OECD;
4) CPTED.

6. Антивирус не только находит зараженные вирусами файлы, но и «лечит» их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние (ПК-15):

1) детектор;
2)доктор;
3) сканер;
4) ревизор;
5) сторож.

7. Секретность зашифрованных сообщений определяется секретностью ключа – это принцип (ПК-15):

1)Кирхгофа;
2) Дирихле;
3) Френеля;
4) Менделеева-Клапейрона.

8. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод (ПК-15):

1) гаммирования;

2) подстановки;
3) кодирования;
4)перестановки;
5) аналитических преобразований.

9. Информация – это ... (ОК-2)

1) содержание упорядоченной последовательности сообщений, отражающих умения и навыки;
2) содержание упорядоченной последовательности сообщений, передающих умения и навыки;
3) содержание упорядоченной последовательности сообщений увеличивающих знания, умения и навыки;
4)содержание упорядоченной последовательности сообщений (в некотором алфавите), отражающих, передающих, увеличивающих знания, умения и навыки.

10. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод (ПК-14):

1) гаммирования;
2) подстановки;
3) кодирования;
4) перестановки;
5) аналитических преобразований.

11. В число универсальных сервисов безопасности входят (ПК-15):

1) Шифрование и туннелирование;
2) Средства построения виртуальных частных сетей
3) Туннелирование

12. Скитала (сцталла) - это:

1)Шифрующее устройство;
2) Заостренное стрекало с острым крюком;
3) Короткое копьё;
4) Криптографическая функция.

13. Интерпретация информации – это (ОК-2):

1)переход к семантическому смыслу;
2) переход к синтаксическому смыслу;
3) расшифровка информации;
4) искажение информации.

14. В число принципов управления персоналом входят (ПК-15):

1) «Разделяй и властвуй»;
2) Разделение обязанностей;
3) Инкапсуляция наследования.

15. Защита информации от утечки это деятельность по предотвращению(ПК-15):

1) Получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником,

владельцем информации прав или правил доступа к защищаемой информации;
2) Воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3) Воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4)Неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5) Несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Тесты к разделу 3

1. Искусственные угрозы безопасности информации вызваны (ПК-14):
1)Деятельностью человека;
2) Ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3) Воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4) Корыстными устремлениями злоумышленников;
5) Ошибками при действиях персонала.

2. Какая категория людей является наиболее рискованной для организации с точки зрения вероятного мошенничества и нарушения безопасности (ОК-2)?
1)Сотрудники организации;
2) Хакеры;
3) Фракеры;
4) Контрагенты (лица, работающие по договору).

3. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности (ПК-14)?
1) Список стандартов, процедур и политик для разработки программы безопасности;
2) Текущая версия ISO 17799;
3) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях;
4)Открытый стандарт, определяющий цели контроля.

4. К посторонним лицам нарушителям информационной безопасности относится (ПК-14):
1) Представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
2) Персонал, обслуживающий технические средства;
3) Технический персонал, обслуживающий здание;

4) Пользователи;
5) Сотрудники службы безопасности;
6)Представители конкурирующих организаций;
7) Лица, нарушившие пропускной режим.

5. Доступность информации – это (ОК-2):

1)Гарантия получения требуемой информации или информационной услуги пользователем за определенное время;
2) Гарантия получения требуемой информации в любое время;
3) Предоставление информационной услуги;
4) Предоставление информации для последующей обработки.

6. Что самое главное должно продумать руководство при классификации данных (ОК-2)?

1) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным;
2)Необходимый уровень доступности, целостности и конфиденциальности;
3) Оценить уровень риска и отменить контрмеры;
4) Управление доступом, которое должно защищать данные.

7. Система формирования режима информационной безопасности – это (ПК-14):

1)Многоуровневая система, обеспечивающая комплексную защиту информационных систем от вредных воздействий, наносящих ущерб субъектам информационных отношений;
2) Многоуровневая система, обеспечивающая комплексную защиту информации с применением криптографических средств;
3) Система, обеспечивающая защиту конфиденциальной информации;
4) Система криптографической защиты информации.

8. Уровни формирования режима информационной безопасности – это (ПК-14):

1) Законодательно-правовой;
2) Административный (организационный);
3) Программно-технический;
4)Все вместе взятое.

9. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод (ПК-15):

1)гаммирования;
2) подстановки;
3) кодирования;
4) перестановки;
5) аналитических преобразований.

10. Перехват данных является угрозой (ОК-2):

1) Доступности;
2) Конфиденциальности;
3) Целостности.

Тесты к разделу 4

1. Что из перечисленного не является целью проведения анализа рисков (ПК-14)?

1)Делегирование полномочий;
2) Количественная оценка воздействия потенциальных угроз;
3) Выявление рисков;
4) Определение баланса между воздействием риска и стоимостью необходимых контрмер.

2. Естественные угрозы безопасности информации вызваны (ПК-15):

1) Деятельностью человека;
2) Ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3)Воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4) Корыстными устремлениями злоумышленников;
5) Ошибками при действиях персонала.

3. Занимается поиском и исследованием математических методов преобразования информации (ОК-2):

1)Криптография;
2) Статистика;
3) Высшая математика.

4. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству (ПК-15)?

1) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования;
2) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации;
3)Улучшить контроль за безопасностью этой информации;
4) Снизить уровень классификации этой информации.

5. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой (ПК-15)?

1) Анализ связующего дерева;
2) AS/NZS;
3) NIST;
4) Анализ сбоев и дефектов.

6. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы (ПК-15):

1)детектор;
2) доктор;
3) сканер;
4) ревизор;

5) сторож.

7. Решетка Кардано – это пример шифра (ПК-15):

1)перестановки;
2) замены;
3) подмены;
4) гаммирования .

8. Какие уровни семиуровневой модели ISO/OSI связаны с сетевым адаптером (ПК-15):

1) Канальный и сетевой;
2)Физический и канальный;
3) Физический и сетевой.

9. Конфиденциальность информации – это (ОК-2):

1)Гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена;
2) Гарантия доступности информации для последующей обработки;
3) Гарантия доступности информации руководству организации;
4) Доступность информации только работникам организации.

10. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска, когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным: (ПК-14)

1) детектор;
2) доктор;
3) сканер;
4)ревизор;
5) сторож.

11. Системы, которые используют два математически связанных друг с другом ключа, называют (ПК-14):

1)асимметричными;
2) симметричным;
3) квадратурными;
4) циклическими.

12. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков (ПК-14)?

1) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски;
2) Когда риски не могут быть приняты во внимание по политическим соображениям;
3) Когда необходимые защитные меры слишком сложны;
4)Когда стоимость контрмер превышает ценность актива и потенциальные потери.

13. Для подтверждения того факта, что данный открытый ключ принадлежит конкретному лицу и никому другому служит (ПК-14):

1)Сертификат;

2) Дайджест;
3) Контрольная сумма.

14. Какого типа бывает информация по отношению к источнику или приемнику (ПК-14):

1)входная, выходная и внутренняя;
2) исходная, промежуточная и результирующая;
3) постоянная, переменная и смешанная;
4) первичная и вторичная.

15. Какая из приведенных техник является самой важной при выборе конкретных защитных мер (ПК-15)?

1) Анализ рисков;
2)Анализ затрат / выгоды;
3) Результаты ALE;
4) Выявление уязвимостей и угроз, являющихся причиной риска.

Тесты к разделу 5

1. Эффективная программа безопасности требует сбалансированного применения (ПК-14):

1)Технических и нетехнических методов;
2) Контрмер и защитных механизмов;
3) Физической безопасности и технических средств защиты;
4) Процедур безопасности и шифрования.

2. Программно-технический уровень включает следующие подуровни (ПК-14):

1)Физический, технический (аппаратный), программный;
2) Физический, технический (аппаратный), экономический;
3) Технический (аппаратный), программный, идеологический;
4) Физический, технический (аппаратный), программный и экономический.

3. Что приводит к уменьшению пропускной способности сети при интенсивном трафике (ПК-14)?

1)Увеличение числа коллизий;
2) Увеличение фрэйма;
3) Уменьшение сечения линии связи.

4. Порт транспортного протокола (называемый также сокетом или сеансом в других протоколах), подобен ... (ПК-14)

1)виртуальному каналу между двумя коммуникационными процессами;
2) витой паре, соединяющей ПЭВМ с сетью;
3) IP-адресу хоста.

5. Алгоритм, преобразующий массив входных данных произвольной длины в (выходную) битовую строку фиксированной длины называют (ПК-15):

1) Хэш-функцией;
2) Бит-функцией;
3) Байт-функцией;

4) Алгоритмом Френеля.

6. Какой уровень стека протоколов TCP/IP определяет маршрут между компьютерами, находящимися в разных сетях (ПК-15)?

1)Сетевой;
2) Транспортный;
3) Физический;
4) Канальный.

7. SNMP – протокол позволяет (ПК-14):

1)управлять конфигурацией оборудования в сети;
2) соединять сетевые приложения;
3) обмениваться служебной информацией маршрутизаторам.

8. Во время войны с галлами Ю.Цезарь (102-44 г. до н.э.) использовал (ОК-2):

1) Шифр замены;
2) Шифр подмены;
3) Шифр перестановки.

Критерии оценки:

Оценивание тестирования.

- от 0 до 49,9 % выполненного решения – неудовлетворительно;
- от 50% до 69,9% – удовлетворительно;
- от 70% до 89,9% – хорошо;
- от 90% до 100% – отлично

6. Фонд оценочных средств промежуточной аттестации по дисциплине

Итоговой формой контроля знаний, умений и навыков по дисциплине является экзамен.

Оценка знаний студентов производится по следующим критериям:
- знание на хорошем уровне содержания вопроса;
- знание на хорошем уровне терминологии дисциплины;
- использование в ответе материала из дополнительной литературы;
- умение привести практический пример использования конкретных приемов и методов по специфике изучаемой дисциплины;
- использование в ответе самостоятельно найденных примеров;
- наличие собственной точки зрения по проблеме и умение ее защитить;
- умение четко, кратко и логически связно изложить материал.

Формой текущего контроля является проверка знаний учащихся с помощью с помощью электронных тестов.

Итоговой формой контроля знаний, умений и навыков по дисциплине в 2 семестре является экзамен. Экзамен проводится в форме собеседования по билетам, которые включают 3 (три) теоретических вопроса. Экзамен предполагает получение студентов одной из оценок по 5-балльной шкале: «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Проведение экзаменов как основной формы проверки знаний студентов предполагает соблюдение ряда условий, обеспечивающих педагогическую эффективность оценочной процедуры. Важнейшие среди них:
1. степень охвата разделов учебной программы и понимание взаимосвязей между ними;
2. глубина понимания существа обсуждаемых конкретных проблем, а также актуальности и практической значимости изучаемой дисциплины;
3. диапазон знания философской литературы;
4. логически корректное, непротиворечивое, последовательное и аргументированное построение ответа на экзамене;
5. уровень самостоятельного мышления с элементами творческого подхода к изложению материала.

Экзаменационные вопросы:

1. Безопасность систем электронного документооборота в банковском учреждении.
2. Безопасность электронного финансового документооборота.
3. Виды реализации Internet угроз (перечислить, пояснить механизмы реализации).
4. Виды реализации программных угроз (перечислить, пояснить механизмы реализации).
5. Дать определение понятию «информационная безопасность». Пояснить составляющие.

6. Дать определение понятию «троянская программа».
7. Дать определение понятию «угроза доступности».
8. Дать определение понятию «угроза конфиденциальности».
9. Дать определение понятию «угроза целостности».
10. Дать определение понятию «угроза».
11. Дать определение понятиям «риск», «управление риском»
12. Защита информации в автоматизированных системах банковских расчетов.
13. Источники угроз безопасности информации.
14. Каковы цели обеспечения информационной безопасности. Дать определение составляющим.
15. Классифицировать способы воздействия угроз.
16. Концепция комплексной системы защиты информации (Схема функций и результатов защиты информации).
17. Криминалистическая характеристика компьютерного преступления. Основные способы совершения компьютерного преступления. Проблемы построение систем защищенного документооборота.
18. Методология создания, организации и обеспечения функционирования систем комплексной защиты информации.
19. Определение информации в задачах информационной безопасности. Автономная информация. Информация воздействия. Информация взаимодействия.
20. Организационно – правовое обеспечение защиты информации. (Организационно- правовая основа, юридические аспекты).
21. Организационные мероприятия по защите конфиденциальной информации.
22. Основные виды технических каналов и источников утечки информации.
23. Перечислить задачи системы антивирусной безопасности.
24. Перечислить и пояснить критерии выбора антивирусных средств.
25. Перечислить цели реагирования на нарушения информационной безопасности.
26. Понятия компьютерного преступления.
27. Пример практического применения механизма ЭЦП.
28. Принципы защиты информации от несанкционированного доступа.
29. Пути и проблемы практической реализации концепции комплексной защиты информации.
30. Системная классификация и общий анализ угроз безопасности информации.
31. Содержание административных мер обеспечения информационной безопасности.
32. Содержание законодательных мер обеспечения информационной безопасности.
33. Содержание и структура понятия «безопасность».
34. Содержание и структура понятия «информационная безопасность».
35. Содержание и структура понятия «обеспечение информационной

безопасности».

36. Требования защищенности СВТ от НСД к информации. Классы и группы защищенности СВТ от НСД.
37. Угрозы безопасности информации.
38. Угрозы доступности.
39. Цели безопасности.
40. Средства, используемые для создания механизмов защиты информации в КИС.
41. Методы поиска и сбора информации.
42. Методика устранения компьютерной информации.
43. Уязвимости Windows.
44. Уязвимости UNIX
45. Защита от копирования переносных носителей.
46. Аппаратные ключи защиты.
47. Современные криптосистемы
48. Виды шифров. Методика кодирования.
49. Навесная защита.
50. Антивирусное программное обеспечение.
51. Особенности защиты информации при работе в сети.
52. Безопасная работа в Internet.
53. Целесообразность усиления обороны.
54. Защита от побочного электромагнитного излучения и наводок.
55. Алгоритмы распределения ключей.

Критерии оценки:

- ***«отлично»*** выставляется студенту, если:
  - даны исчерпывающие и обоснованные ответы на все поставленные вопросы, правильно решены практические задания;
  - при ответах выделялось главное, все теоретические положения умело увязывались с требованиями руководящих документов;
  - ответы были четкими и краткими, а мысли излагались в логической последовательности;
  - показано умение самостоятельно анализировать факты, события, явления, процессы в их взаимосвязи и диалектическом развитии.
- ***«хорошо»:***
  - даны полные, достаточно обоснованные ответы на поставленные вопросы, правильно решены практические задания;
  - при ответах не всегда выделялось главное, отдельные положения недостаточно увязывались с требованиями руководящих документов;
  - ответы в основном были краткими, но не всегда четкими и по существу.
- ***«удовлетворительно»:***
  - даны в основном правильные ответы на все поставленные вопросы, но без должной глубины и обоснования;

- на уточняющие вопросы даны правильные ответы;
- при ответах не выделялось главное;
- ответы были многословными, нечеткими и без должной логической последовательности;
- на отдельные дополнительные вопросы не даны положительные ответы.

- **«неудовлетворительно»:**
  - даны неправильные ответы на большинство вопросов;
  - путается в определениях и понятиях;
  - не владеет практическими навыками решения задач.

7. Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. Артемов, А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.– Электрон. текстовые данные.– Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.– 256 с..– Режим доступа: http://www.iprbookshop.ru/33430.– ЭБС «IPRbooks», по паролю
2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.– Электрон. текстовые данные.– Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.– 113 с.– Режим доступа: http://www.iprbookshop.ru/43183.– ЭБС «IPRbooks», по паролю
3. Шаньгин, В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.– Электрон. текстовые данные.– М.: ДМК Пресс, 2014.– 702 с.– Режим доступа: http://www.iprbookshop.ru/29257.– ЭБС «IPRbooks», по паролю
4. Гафнер, В.В. Информационная безопасность [Текст]: учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.–324 с.

Дополнительная литература:

1. Башлы, П.Н. Информационная безопасность [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.– Электрон. текстовые данные.– М.: Евразийский открытый институт, 2012.– 311 с.– Режим доступа: http://www.iprbookshop.ru/10677.– ЭБС «IPRbooks», по паролю
2. Петров, С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.– Электрон. текстовые данные.– Саратов: Ай Пи Ар Букс, 2015.– 326 с.– Режим доступа: http://www.iprbookshop.ru/33857.– ЭБС «IPRbooks», по паролю

Интернет-ресурсы:

1. Википедия – http://ru.wikipedia.org
2. Интернет-портал образовательных ресурсов по ИТ – http://www.intuit.ru
3. Информационный портал по защите информации – http://all-ib.ru
4. Портал с ресурсами по алгоритмике и защите информации – http://algolist.manual.ru
5. Сайт нормативных документов, предоставляемых компанией «Консультант плюс» – www.consultant.ru
6. Электронно-библиотечная система IPRbooks URL: http://www.iprbookshop.ru/. ООО «Ай Пи Эр Медиа». Государственный контракт №1066/15 от 26.02.2015г. на 5000 (пять тысяч) доступов.

7. Научная электронная библиотека – elibrary.ru

РЯДЧЕНКО ВИКТОР ПЕТРОВИЧ
БАШИЕВА АНЖЕЛА ХАМИДОВНА
БОСТАНОВА ЛАУРА КЕМАЛОВНА

КОМПЛЕКСНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебно-методическое пособие для магистрантов 1 курса направления подготовки 09.04.03 Прикладная информатика

Печатается в редакции автора

Корректор
Редактор

Сдано в набор
Формат 60х84/16
Бумага офсетная.
Печать офсетная.
Усл. печ. л.
Заказ №
Тираж

Оригинал-макет подготовлен в Библиотечно-издательском центре СевКавГГТА

369000, г. Черкесск, ул. Ставропольская, 36