Бостанова Л.К.
Рядченко В.П.

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ И СРЕДЫ

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 ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ ГУМАНИТАРНО-ТЕХНОЛОГИЧЕСКАЯ АКАДЕМИЯ

Бостанова Л.К.
Рядченко В.П.

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ И СРЕДЫ

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

Черкесск, 2015

УДК 004.05
ББК 32.97
Б-75

Рассмотрено на заседании кафедры информатики и ИТ
Протокол № 15 от «3» июня 2015 г.
Рекомендовано к изданию редакционно-издательским советом СевКавГГТА.
Протокол № 9 от « 25 » июня 2015 г.

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

Б-75 Бостанова Л.К. Защищенные информационные системы и среды: учебно-методическое пособие для магистрантов 1 курса направления подготовки 09.04.03 Прикладная информатика / Л.К. Бостанова, Рядченко В.П. – Черкесск: БИЦ СевКавГГТА, 2015. – 2 п.л
.

В учебном пособии сформированы рекомендации для усвоения магистрантами учебного материала по курсу «Защищенные информационные системы и среды», предлагаются методические рекомендации к лекционным и практическим занятиям, к самостоятельной работе, а также тестовые задания, что позволит оптимально организовать процесс изучения данной дисциплины.

УДК 004.05
ББК 32.97

СОДЕРЖАНИЕ

Введение

К современному специалисту общество предъявляет достаточно широкий перечень требований, среди которых немаловажное значение имеет наличие у выпускников определенных способностей и умения самостоятельно получать знания из различных источников, систематизировать полученную информацию, давать оценку конкретной ситуации.

Курс «Защищенные информационные системы и среды» направлен на освоение магистрантами основных понятий защиты информационных систем и сред.

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, тестовые задания.

1. Цели и задачи изучения дисциплины

Целями освоения дисциплины «Защищенные информационные системы и среды» является формирование у студентов теоретических основ защиты информации, связанных с созданием и изучением современных защищенных информационных систем различного применения и степени сложности, предотвращением ущерба пользователю информации.

При этом задачами дисциплины являются:

-изучение современной классификации средств защиты информации в корпоративных вычислительных сетях и системах;

- изучение современных технологий построения безопасных информационных систем

- изучение этапов и технологий проектирования и создания безопасных информационных систем;

- изучение современных программных и аппаратных средств защиты информации;

- изучение основных угроз информации в современных информационных системах и сетях;

- изучение инструментальных программных и аппаратных средств анализа защищенности информационных систем и сетей;

- формирование умений в разработке проектов комплексных защищенных инфраструктур для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности, выполняемых с использованием современных программных, программно-аппаратных и аппаратных средств защиты информации;

- формирование навыков разработки и внедрения комплексной защищенной инфраструктуры на предприятиях, включающих навыки базовой и расширенной настройки и использования современных программных и аппаратных средств защиты информации: файрволлов, интерактивных детекторов атак, защищенных доменных сервисов.

Дисциплина «Защищенные информационные системы и среды» относится к дисциплинам по выбору студента вариативной части Блока 1 (Б1.В.ДВ.2.1), имеет тесную связь с другими дисциплинами.

Планируемые результаты освоения образовательной программы (ОП) – компетенции обучающихся определяются требованиями стандарта по направлению подготовки (специальности) 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.	ОПК-5	Способность на практике применять новые научные принципы и методы исследований	**Знать:** современные технологии построения безопасных информационных систем; основные угрозы информационной безопасности и возможные пути их разрешения. **Уметь:** анализировать и оценивать угрозы информационной безопасности; применять отечественные и зарубежные стандарты в области компьютерной безопасности. **Владеть:** навыками организации и обеспечения режима секретности информационных систем.
2.	ПК-2	Способность формализовывать задачи прикладной области, при решении которых возникает необходимость использования количественных и качественных оценок	**Знать:** принципы построения информационных систем; методы организационной защиты информации. **Уметь:** предотвращать нарушения сетевой безопасности с использованием различных программных и аппаратных средств защиты; оценивать защищенность информационных систем. **Владеть:** методами формирования требований по защите информации.
3.	ПК-14	Способность принимать эффективные проектные решения в условиях неопределенности и риска	**Знать:** классификацию рисков по уровням защиты и фазам жизненного цикла ИС. **Уметь:** принимать решения по безопасности информатизации предприятий в условиях неопределенности и риска. **Владеть:** навыками управления рисков на этапах проектирования защищенных информационных систем; количественными, качественными и комбинированными методами оценки рисков.

В результате изучения дисциплины магистрант должен усвоить:

- угрозы безопасности, системы защиты информационных систем и сред;

- уязвимость основных структурно-функциональных элементов информационных систем;
- классификацию каналов проникновения в информационную систему и утечки информации;
- защиту файлов, контроль доступа, уязвимость паролей;
- обеспечение надежного бесперебойного доступа к данным и приложениям, защита от вирусов, спама и внешних атак.

2. Лекции

Для понимания лекционного материала и качественного его усвоения студентам необходимо вести конспекты лекций. В течение лекции студент делает пометки по тем вопросам лекции, которые требуют уточнений и дополнений. Вопросы, которые преподаватель не отразил в лекции, студент должен изучать самостоятельно.

Содержание лекций

Тема 1. **Угрозы безопасности информации.**
Угрозы безопасности информации, АС и субъектов информационных отношений, источники угроз безопасности, классификация угроз безопасности, основные преднамеренные и непреднамеренные угрозы.

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.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

Дополнительная литература:

1.Гафнер, В.В. Информационная безопасность [Текст]: учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.

Тема 2. Модели угроз и нарушителей информационной безопасности .
Уязвимость, угроза ИБ, источник угрозы ИБ, модель угроз ИБ, модель нарушителя ИБ. Информационная инфраструктура. Причины уязвимости 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.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

Дополнительная литература:

1.Гафнер, В.В. Информационная безопасность [Текст]: учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.

Тема 3. **Классификация каналов проникновения в систему и утечки информации.**

Прямые и косвенные каналы проникновения в систему и утечки информации. Физические, электромагнитные, информационные каналы.

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.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

Дополнительная литература:

1.Гафнер, В.В. Информационная безопасность [Текст]: учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.

Тема 4. Основные защитные механизмы операционной системы.

Идентификация и аутентификация пользователя при входе в систему; разграничение прав доступа к файловой системе, в основе которого лежит реализация дискреционной модели доступа; аудит. Принципиальные недостатки защитных механизмов, используемых в операционных системах.

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.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

Дополнительная литература:

1.Гафнер, В.В. Информационная безопасность [Текст]: учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.

Тема 5. Средства защиты открытых информационных систем.

Сервисы безопасности. Средства обеспечения ИБ в сетях. Их назначение, особенности применения и примеры. Аутентификация в сетях: обычные и одноразовые пароли; серверы аутентификации. Дополнительная информация и итоговые рекомендации по защите открытых 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.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

Дополнительная литература:

1.Гафнер, В.В. Информационная безопасность [Текст]: учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.

Тема 6. Система безопасности Windows.

Параметры безопасности. Настройка операционной системы Windows. Права пользователей и система управления доступом. Квалификация пользователей. Средства защиты.

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.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

Дополнительная литература:

1.Гафнер, В.В. Информационная безопасность [Текст]: учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.

Тема 7. Обеспечение надежности и бесперебойного функционирования информационных систем среды

Слабости системных утилит, команд и сетевых сервисов на примере стека протоколов tcp/ip (Telnet, FTP, NFS, DNS, NIS, World Wide Web, команды удаленного выполнения, Sendmail и электронная почта, другие утилиты). Средства замены уязвимых сервисов TCP/IP. Слабости современных технологий программирования (Java, ActiveX…) и ошибки в программном обеспечении. Сетевые вирусы. Виды угроз ресурсам интранета и Интернета.

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.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

Дополнительная литература:

1.Гафнер, В.В. Информационная безопасность [Текст]: учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.

3.Практические занятия

При подготовке к практическим занятиям следует использовать основную литературу из представленного списка рабочей программе, а также руководствоваться приведенными указаниями. Для наиболее глубокого освоения дисциплины рекомендуется изучать литературу, обозначенную как «Дополнительная» в представленном списке.

На практических занятиях рекомендуется принимать активное участие в обсуждении проблем, возникающих при решении учебных задач, развивать способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем по тематике практических занятий.

Магистранту рекомендуется следующая схема подготовки к практическому занятию:

- проработка конспекта лекций;
- чтение рекомендованной основной и дополнительной литературы по изучаемому разделу дисциплины;
- решение домашних задач;
  при выполнении упражнения или задачи нужно сначала понять, что требуется в задаче, какой теоретический материал нужно использовать, наметить план решения задачи;

- при возникновении затруднений следует сформулировать конкретные вопросы к преподавателю.

Содержание практических занятий.
Практическое занятие № 1.
Тема 1. Каналы утечки информации в современных автоматизированных системах электронной обработки данных.
Цель занятия: Ознакомление с основными каналами утечки информации
Вопросы для обсуждения:

1. Сканирование уязвимостей. Тестирование проникновения.
2. Удаленное администрирование web-сервера

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.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

Дополнительная литература:

1.Гафнер, В.В. Информационная безопасность [Текст]: учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.

Практическое занятие № 2.
Тема 2. Классификация внутренних и внешних нарушителей
Цель занятия: Изучение внутренних и внешних нарушителей
Вопросы для обсуждения:

1. Определение угроз безопасности информации в информационной системе.
2. Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации.

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.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

Дополнительная литература:

1.Гафнер, В.В. Информационная безопасность [Текст]: учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.

Практическое занятие № 3.

Тема 3. Технологии аутентификации и шифрования

Цель занятия: Изучение основных понятий аутентификации и шифрования

Вопросы для обсуждения:

1. Защита обратной связи при вводе аутентификационной информации
2. Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

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.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

Дополнительная литература:

1.Гафнер, В.В. Информационная безопасность [Текст]: учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.

Практическое занятие № 4.

Тема 4. Безопасность web-ориентированного контента

Цель занятия: Изучение и обеспечение безопасности web-содержимого.

Вопросы для обсуждения:

1. Опубликование информации на web-сайтах.
2. Обеспечение безопасности технологий создания активного содержимого сайта. URLs и cookies.

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.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

Дополнительная литература:

1.Гафнер, В.В. Информационная безопасность [Текст]: учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.

4. Самостоятельная работа

Самостоятельная работа магистрантов – способ активного, целенаправленного приобретения новых для него знаний и умений, выполняемый во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Целью самостоятельной работы магистрантов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного, исследовательского и профессионального уровня. Самостоятельная работа не регламентируется расписанием.

Видами заданий для самостоятельной работы могут быть: - для овладения знаниями: чтение текста (учебника, первоисточника, дополнительной литературы); составление плана текста и конспектирование текста; работа со словарями и справочниками; ознакомление с нормативными документами; использование аудио- и видеозаписей, компьютерной техники и Интернета и др.; - для закрепления и систематизации знаний: работа с конспектом лекции (обработка текста); повторная работа над учебным материалом; составление плана и тезисов ответа, с учетом перечня вопросов, выносимых на семинарские занятия; ответы на контрольные вопросы; подготовка сообщений к выступлению на семинаре; подготовка докладов; составление библиографии, и др.

При подготовке вопросов важно:

- использовать достаточно широкий диапазон массива информации, провести обзор периодической литературы и специальных изданий, составить каталог Интернет-ресурсов;
- представить различные подходы, четко и полно определить рассматриваемые понятия, выявить взаимосвязи понятий и явлений, взаимозависимости и связи с другими вопросами;
- грамотно структурировать материал, ясно, четко и логично его излагать, приводить соответствующие примеры из практики, для иллюстрации положений, тезисов и выводов использовать таблицы, схемы, графики;
- отработать решение типовых заданий;
- подготовить презентацию.

Если в процессе самостоятельной работы над изучением теоретического материала или при решении задач у магистранта возникают вопросы,

разрешить которые самостоятельно не удается, необходимо обратиться к преподавателю для получения у него разъяснений или указаний. В своих вопросах магистрант должен четко выразить, в чем он испытывает затруднения, характер этого затруднения. За консультацией следует обращаться и в случае, если возникнут сомнения в правильности ответов на вопросы самопроверки.

Подготовка презентации и доклада

Презентация, согласно толковому словарю русского языка Д.Н. Ушакова: «… способ подачи информации, в котором присутствуют рисунки, фотографии, анимация и звук». Для подготовки презентации рекомендуется использовать: PowerPoint, MS Word, Acrobat Reader, LaTeX-овский пакет beamer. Самая простая программа для создания презентаций – Microsoft PowerPoint. Для подготовки презентации необходимо собрать и обработать начальную информацию.

Последовательность подготовки презентации:

1. Четко сформулировать цель презентации: вы хотите свою аудиторию мотивировать, убедить, заразить какой-то идеей или просто формально отчитаться.

2. Определить каков будет формат презентации: живое выступление (тогда, сколько будет его продолжительность) или электронная рассылка (каков будет контекст презентации).

3. Отобрать всю содержательную часть для презентации и выстроить логическую цепочку представления.

4. Определить ключевые моменты в содержании текста и выделить их.

5. Определить виды визуализации (картинки) для отображения их на слайдах в соответствии с логикой, целью и спецификой материала.

6. Подобрать дизайн и форматировать слайды (количество картинок и текста, их расположение, цвет и размер).

7. Проверить визуальное восприятие презентации.

К видам визуализации относятся иллюстрации, образы, диаграммы, таблицы. Иллюстрация - представление реально существующего зрительного ряда. Образы – в отличие от иллюстраций - метафора. Их назначение - вызвать эмоцию и создать отношение к ней, воздействовать на аудиторию. С помощью хорошо продуманных и представляемых образов, информация может надолго остаться в памяти человека. Диаграмма - визуализация количественных и качественных связей. Их используют для убедительной демонстрации данных, для пространственного мышления в дополнение к логическому. Таблица - конкретный, наглядный и точный показ данных. Ее основное назначение - структурировать информацию, что порой облегчает восприятие данных аудиторией.

Практические советы по подготовке презентации готовьте отдельно:

- печатный текст + слайды + раздаточный материал;
- слайды - визуальная подача информации, которая должна содержать минимум текста, максимум изображений, несущих смысловую нагрузку, выглядеть наглядно и просто;

- текстовое содержание презентации – устная речь или чтение, которая должна включать аргументы, факты, доказательства и эмоции;
- рекомендуемое число слайдов 17-22;
- обязательная информация для презентации: тема, фамилия и инициалы выступающего; план сообщения; краткие выводы из всего сказанного; список использованных источников;
- раздаточный материал – должен обеспечивать ту же глубину и охват, что и живое выступление: люди больше доверяют тому, что они могут унести с собой, чем исчезающим изображениям, слова и слайды забываются, а раздаточный материал остается постоянным осязаемым напоминанием; раздаточный материал важно раздавать в конце презентации; раздаточный материалы должны отличаться от слайдов, должны быть более информативными.

Тема доклада должна быть согласованна с преподавателем и соответствовать теме учебного занятия. Материалы при его подготовке, должны соответствовать научно-методическим требованиям вуза и быть указаны в докладе. Необходимо соблюдать регламент, оговоренный при получении задания. Иллюстрации должны быть достаточными, но не чрезмерными.

Работа студента над докладом-презентацией включает отработку умения самостоятельно обобщать материал и делать выводы в заключении, умения ориентироваться в материале и отвечать на дополнительные вопросы слушателей, отработку навыков ораторства, умения проводить диспут.

Докладчики должны знать и уметь: сообщать новую информацию; использовать технические средства; хорошо ориентироваться в теме всего семинарского занятия; дискутировать и быстро отвечать на заданные вопросы; четко выполнять установленный регламент (не более 10 минут); иметь представление о композиционной структуре доклада и др.

Структура выступления

Вступление помогает обеспечить успех выступления по любой тематике. Вступление должно содержать: название, сообщение основной идеи, современную оценку предмета изложения, краткое перечисление рассматриваемых вопросов, живую интересную форму изложения, акцентирование внимания на важных моментах, оригинальность подхода.

Основная часть, в которой выступающий должен глубоко раскрыть суть затронутой темы, обычно строится по принципу отчета. Задача основной части – представить достаточно данных для того, чтобы слушатели заинтересовались темой и захотели ознакомиться с материалами. При этом логическая структура теоретического блока не должны даваться без наглядных пособий, аудио-визуальных и визуальных материалов.

Заключение – ясное, четкое обобщение и краткие выводы, которых всегда ждут слушатели

Темы для докладов по дисциплине «Защищенные информационные системы и среды»

1. Применение защищенных информационных систем среды.
2. Выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию.
3. Методы и средства защиты информационных систем.
4. Проблема оценки защищенности информационных систем среды.
5. Виртуальная консолидация данных.
6. Способы хранения информации.
7. Интеллектуальные дисковые массивы.
8. Криптографическая защита информации.
9. Требования к аутентификации и шифрованию.
10. Классификация информации по уровню конфиденциальности. Реквизиты документов.
11. Защита каналов утечки. Мониторинг (аудит) действий пользователей. Классификация внутренних нарушителей
12. Нетехнические меры защиты от внутренних угроз.
13. Психологические меры. Организационные меры
14. Персональные firewall'bi и персональные устройства firewall'a
15. VPN и Dial-in серверы. Внутренние серверы. DNS-серверы. SMTP-серверы.
16. Основные характеристики пакетных фильтров в ОС FreeBSD.
17. Определение злоупотреблений. Определение аномалий. Возможные ответные действия IDS.
18. Системы Honey Pot и Padded Cell. Выбор IDS. Определение окружения IDS.
19. Авторитетные name-серверы. Кэширующие name-серверы. Resolver'bi.
20. Безопасное инсталлирование и конфигурирование ОС
21. Обеспечение безопасности технологий создания активного содержимого. URLs и cookies.
22. Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе.
23. Автоматизированные инструментальные средства анализа лог-файлов

Критерии оценки:

- *оценка «зачтено» выставляется студенту, если*:

- тема соответствует содержанию доклада;
- широкий круг и адекватность использования литературных источников по проблеме;
- правильное оформление ссылок на используемую литературу;
- основные понятия проблемы изложены достаточно полно и глубоко;
- отмечена грамотность и культура изложения;
- соблюдены требования к оформлению и объему доклада;

- материал систематизирован и структурирован;
- сделаны обобщения и сопоставления различных точек зрения по рассматриваемому вопросу;
- сделаны и аргументированы основные выводы;
- отчетливо видна самостоятельность суждений;

- *оценка «не зачтено»:*

- содержание не соответствует теме;
- литературные источники выбраны не по теме, не актуальны;
- нет ссылок на использованные источники информации;
- тема не раскрыта;
- в изложении встречается большое количество орфографических и стилистических ошибок;
- требования к оформлению и объему материала не соблюдены;
- структура доклада не соответствует требованиям методических указаний;
- не проведен анализ материалов доклада;
- нет выводов.

5. Фонд оценочных средств для проведения текущего контроля

Список вопросов для проведения текущего контроля и устного опроса обучающихся:

Вопросы к разделу 1.

- Угрозы безопасности информации.
- Архитектуры системы защиты: особенности современных АС как объекта защиты
- Источники угроз безопасности,
- Классификация угроз безопасности,
- Основные преднамеренные и непреднамеренные искусственные угрозы

Вопросы к разделу 2.

- Уязвимость, угроза ИБ
- Источник угрозы ИБ
- Модель угроз ИБ
- Модель нарушителя ИБ.
- Информационная инфраструктура.
- Причины уязвимости ИС

Вопросы к разделу 3.

- Прямые и косвенные каналы проникновения в систему и утечки информации.

- Физические, электромагнитные, информационные каналы

Вопросы к разделу 4.

- Идентификация и аутентификация пользователя при входе в систему.
- Разграничение прав доступа к файловой системе, в основе которого лежит реализация дискреционной модели доступа;
- Аудит.
- Принципиальные недостатки защитных механизмов операционной системы семейства Unix

Вопросы к разделу 5.

- Сервисы безопасности.
- Средства обеспечения ИБ в сетях. Их назначение, особенности применения и примеры.
- Аутентификация в сетях: обычные и одноразовые пароли; серверы аутентификации.
  Дополнительная информация и итоговые рекомендации по защите открытых ИС.

Вопросы к разделу 6.

- Параметры безопасности.
- Настройка операционной системы Windows.
- Права пользователей и система управления доступом.
- Квалификация пользователей.
- Средства защиты

Вопросы к разделу 7.

- Слабости системных утилит, команд и сетевых сервисов на примере стека протоколов tcp/ip (Telnet, FTP, NFS, DNS, NIS, World Wide Web.
- команды удаленного выполнения, Sendmail и электронная почта, другие утилиты.
- Средства замены уязвимых сервисов TCP/IP.
- Слабости современных технологий программирования (Java, ActiveX…) и ошибки в программном обеспечении.
  Сетевые вирусы.
  Виды угроз ресурсам интранета и Интернета

  Критерии оценки:
  - *оценка «отлично» выставляется студенту, если:*

- даны исчерпывающие и обоснованные ответы на все поставленные вопросы, правильно;
- 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;

- *оценка «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.
- оценка «*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.
- *оценка «неудовлетворительно»:*
  - не выполнены требования, предъявляемые к знаниям, оцениваемым “удовлетворительно”.

Тестовые задания к проведению текущего контроля по дисциплине

«Защищенные информационные системы и среды»

<u>Тесты к разделу 1</u>

1. 1. Выделите верное утверждение в отношении информационной безопасности. (ОПК-5)

(Отметьте один правильный вариант ответа.)

наступление нового этапа развития ИТ приводит к быстрому падению уровня информационной безопасности;
наступление нового этапа развития ИТ приводит к быстрому повышению уровня информационной безопасности;
уровень информационной безопасности не зависит от этапов развития ИТ

2. К какому уровню обеспечения ИБ относится «Доктрина информационной безопасности Российской Федерации»? (ОПК-5)

(Отметьте один правильный вариант ответа.)

административный;
научно-технический;
законодательный;
процедурный.
3. К какому уровню обеспечения ИБ относится «Политика информационной безопасности», утвержденная руководителем в конкретной организации? (ОПК-5)

(Отметьте один правильный вариант ответа.)
научно-технический
процедурный
административный
законодательный
4. Выделите основные составляющие информационной безопасности. (ОПК-5)

(Ответ считается верным, если отмечены все правильные варианты ответов.)
целостность
доступность
полнота
конфиденциальность
актуальность

5. Какой аспект информационной безопасности отражает возможность за приемлемое время получить требуемую информационную услугу? (ОПК-5)

(Отметьте один правильный вариант ответа.)
конфиденциальность
доступность
целостность
6. Если в результате DoS-атаки злоумышленников сайт перестал работать, какой аспект информационной безопасности был нарушен? (ПК-2)
(Отметьте один правильный вариант ответа.)

целостность
конфиденциальность
доступность
7. Какой аспект ИБ наиболее актуален для научно-исследовательских организаций, имеющих открытые Web-серверы? (ПК-2)

(Отметьте один правильный вариант ответа.)
конфиденциальность
доступность
целостность
8. К какой угрозе можно отнести возможность ситуации, когда уволенный сотрудник беспрепятственно пользуется служебными полномочиями, в том числе корпоративным доступом в Интернет? (ПК-14)

(Отметьте один правильный вариант ответа.)
вредоносные программы
действия инсайдеров
хакерские атаки
спам
9. Как называются атаки, направленные на выведение из строя того или иного узла сети? (ПК-2)
(Отметьте один правильный вариант ответа.)
Virus
Spam
DoS
Worm
10. Как называется модель, описывающая вероятный облик злоумышленника, т. е. его квалификацию, имеющиеся средства для реализации тех или иных атак, обычное время действия и т. п? (ОПК-5)
(Отметьте один правильный вариант ответа.)
модель угрозы
модель нарушителя
модель безопасности
модель уязвимости

Тесты к разделу 2

1. Какой термин определяет защищенность жизненно важных интересов государственного или коммерческого предприятия от внутренних и внешних угроз, защиту кадрового и интеллектуального потенциала, технологий, данных и информации, капитала и прибыли, которая обеспечивается системой мер правового, экономического, организационного, информационного, инженерно-технического и социального характера? (ОПК-5)

(Отметьте один правильный вариант ответа.)
информационная безопасность
корпоративная безопасность
стратегическая безопасность
экономическая безопасность

2. Какой аспект ИБ наиболее актуален для провайдера Интернет-услуг? (ПК-2)

(Отметьте один правильный вариант ответа.)

конфиденциальность
доступность
целостность
3. Кто такой инсайдер? (ОПК-5)
(Отметьте один правильный вариант ответа.)

человек, разработавший вредоносную программу

внутренний злоумышленник
человек, подвергшийся атаке злоумышленника
внешний злоумышленник
4 Совокупность нескольких базовых стандартов с чётко определёнными подмножествами обязательных и факультативных возможностей, предназначенная для реализации заданной функции или группы функций называется (ОПК-5)
профилем
срезом
группой стандартов
системой требований
5 Согласно ISO 12207, объединение одного или нескольких процессов, аппаратных средств, программного обеспечения, оборудования и людей для удовлетворения определённым потребностям или целям это
система
информационная система
полнофункциональный программно-аппаратный комплекс
вычислительный центр
6 В стандарте ISO 12207 описаны _____ основных процессов жизненного цикла программного обеспечения (ОПК-5)
три
четыре
пять
шесть

Тесты к разделу 3

1. Согласно ISO 12207, процессы, протекающие во время жизненного цикла программного обеспечения, дожны быть совместимы с процессами, протекающими во время жизненного цикла (ОПК-5)
автоматизированной системы
информационной системы
компьютерной системы
системы обработки и передачи данных

2 Согласно стандарту ISO 12207 основным процессом жизненного цикла программного обеспечения является (ОПК-5)
приобретение
решение проблем
обеспечение качества
аттестация
3 Согласно стандарту ISO 12207 основным процессом жизненного цикла программного обеспечения является (ОПК-5)
процесс поставки
документирования
аудит

управление конфигурацией
4 Согласно стандарту ISO 12207 основным процессом жизненного цикла программного обеспечения является (ОПК-5)
сопровождение
управление
создание инфраструктуры
обучение
5 Согласно стандарту ISO 12207 основным процессом жизненного цикла программного обеспечения является (ОПК-5)
функционирование
управление
обеспечение качества
документирование
6 Согласно стандарту ISO 12207 вспомогательным процессом жизненного цикла программного обеспечения является (ОПК-5)
обеспечение качества
усовершенствование
обучение
создание инфраструктуры
7 Согласно стандарту ISO 12207 вспомогательным процессом жизненного цикла программного обеспечения является (ОПК-5)
аттестация
приобретение
поставка
сопровождение
8 Согласно стандарту ISO 12207 вспомогательным процессом жизненного цикла программного обеспечения является (ОПК-5)
совместная оценка
усовершенствование
обучение
создание инфраструктуры
9 Согласно стандарту ISO 12207 вспомогательным процессом жизненного цикла программного обеспечения является (ОПК-5)
решение проблем
аудит
сопровождение
усовершенствование
10 Согласно стандарту ISO 12207 вспомогательным процессом жизненного цикла программного обеспечения является (ОПК-5)
верификация
управление конфигурацией
создание инфраструктуры
процесс поставки

11 Согласно стандарту ISO 12207 организационным процессом является (ОПК-5)
усовершенствование
согласование сроков
разработка технического задания
согласование качественных показателей
12 Основные угрозы доступности информации: (ПК-14)
непреднамеренные ошибки пользователей
злонамеренное изменение данных
хакерская атака
отказ программного и аппаратно обеспечения
разрушение или повреждение помещений
перехват данных

Тесты к разделу 4

1. Суть компрометации информации (ПК-14)
внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации;
несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений;
внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений.
2. Информационная безопасность автоматизированной системы – это состояние (ПК-2)
автоматизированной системы, при котором она, …
с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды;
с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации;
способна противостоять только информационным угрозам, как внешним так и внутренним;
способна противостоять только внешним информационным угрозам.
3. Методы повышения достоверности входных данных: (ПК-2)
замена процесса ввода значения процессом выбора значения из предлагаемого множества;
отказ от использования данных;
проведение комплекса регламентных работ;
использование вместо ввода значения его считывание с машиночитаемого носителя;

введение избыточности в документ первоисточник;
многократный ввод данных и сличение введенных значений.
4. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ) (ПК-2)
МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения;
МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты;
МЭ работают только на сетевом уровне, а СОВ – еще и на физическом.
5. Сервисы безопасности: (ПК-14)
идентификация и аутентификация
шифрование
инверсия паролей
контроль целостности
регулирование конфликтов
экранирование
обеспечение безопасного восстановления
кэширование записей
6. Под угрозой удаленного администрирования в компьютерной сети понимается угроза (ПК-14)
несанкционированного управления удаленным компьютером;
внедрения агрессивного программного кода в рамках активных объектов Web-страниц;
перехвата или подмены данных на путях транспортировки;
вмешательства в личную жизнь;
поставки неприемлемого содержания.

Тесты к разделу 5

1. Причины возникновения ошибки в данных: (ПК-14)
погрешность измерений
ошибка при записи результатов измерений в промежуточный документ
неверная интерпретация данных
ошибки при переносе данных с промежуточного документа в компьютер
использование недопустимых методов анализа данных
неустранимые причины природного характера
преднамеренное искажение данных
ошибки при идентификации объекта или субъекта хозяйственной деятельности
2. К формам защиты информации не относится: (ОПК-5)
аналитическая
правовая
организационно-техническая
страховая
3. Наиболее эффективное средство для защиты от сетевых атак (ПК-14)
использование сетевых экранов или «firewall»

использование антивирусных программ
посещение только «надёжных» Интернет-узлов
использование только сертифицированных программ-броузеров при доступе к сети Интернет

4. Информация, составляющая государственную тайну не может иметь гриф (ОПК-5)
«для служебного пользования»
«секретно»
«совершенно секретно»
«особой важности»

5. Разделы современной криптографии: (ОПК-5)
симметричные криптосистемы
криптосистемы с открытым ключом
криптосистемы с дублированием защиты
системы электронной подписи
управление паролями
управление передачей данных
управление ключами

6. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности: (ОПК-5)
рекомендации X.800
Оранжевая книга
Закону «Об информации, информационных технологиях и о защите информации»

7. Утечка информации – это …(ОПК-5)
несанкционированный процесс переноса информации от источника к злоумышленнику;
процесс раскрытия секретной информации
процесс уничтожения информации
непреднамеренная утрата носителя информации

8. Основные угрозы конфиденциальности информации: (ОПК-5)
маскарад
карнавал
переадресовка
перехват данных
блокирование
злоупотребления полномочиями

9. Элементы знака охраны авторского права: (ОПК-5)
буквы С в окружности или круглых скобках
буквы Р в окружности или круглых скобках
наименования (имени) правообладателя
наименование охраняемого объекта
года первого выпуска программы

10. Защита информации обеспечивается применением антивирусных средств (ПК-2)
да
нет
не всегда
11. Средства защиты объектов файловой системы основаны на… (ПК-14)
определении прав пользователя на операции с файлами и каталогами;
задании атрибутов файлов и каталогов, независящих от прав пользователей.
12. Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование – … угроза (ОПК-5)
активная
пассивная
13. Преднамеренная угроза безопасности информации (ОПК-5)
кража
наводнение
повреждение кабеля, по которому идет передача, в связи с погодными условиями
ошибка разработчика
14. Концепция системы защиты от информационного оружия не должна включать (ОПК-5)
средства нанесения контратаки с помощью информационного оружия;
механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры;
признаки, сигнализирующие о возможном нападении;
процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей.

Тесты к разделу 6

1. Причины возникновения ошибки в данных: (ПК-14)
погрешность измерений
ошибка при записи результатов измерений в промежуточный документ
неверная интерпретация данных
ошибки при переносе данных с промежуточного документа в компьютер
использование недопустимых методов анализа данных
неустранимые причины природного характера
преднамеренное искажение данных
ошибки при идентификации объекта или субъекта хозяйственной деятельности
2. К формам защиты информации не относится: (ОПК-5)
аналитическая
правовая
организационно-техническая
страховая
3. Наиболее эффективное средство для защиты от сетевых атак (ПК-14)

использование сетевых экранов или «firewall»
использование антивирусных программ
посещение только «надёжных» Интернет-узлов
использование только сертифицированных программ-броузеров при доступе к сети Интернет
4. Информация, составляющая государственную тайну не может иметь гриф (ОПК-5)
«для служебного пользования»
«секретно»
«совершенно секретно»
«особой важности»
5. Разделы современной криптографии: (ОПК-5)
симметричные криптосистемы
криптосистемы с открытым ключом
криптосистемы с дублированием защиты
системы электронной подписи
управление паролями
управление передачей данных
управление ключами
6. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности: (ОПК-5)
рекомендации X.800
Оранжевая книга
Закону «Об информации, информационных технологиях и о защите информации»
7. Утечка информации – это …(ОПК-5)
несанкционированный процесс переноса информации от источника к злоумышленнику;
процесс раскрытия секретной информации
процесс уничтожения информации
непреднамеренная утрата носителя информации
8. Основные угрозы конфиденциальности информации: (ОПК-5)
маскарад
карнавал
переадресовка
перехват данных
блокирование
злоупотребления полномочиями
9. Элементы знака охраны авторского права: (ОПК-5)
буквы С в окружности или круглых скобках
буквы Р в окружности или круглых скобках
наименования (имени) правообладателя
наименование охраняемого объекта

года первого выпуска программы
10. Защита информации обеспечивается применением антивирусных средств (ПК-2)
да
нет
не всегда
11. Средства защиты объектов файловой системы основаны на… (ПК-14)
определении прав пользователя на операции с файлами и каталогами;
задании атрибутов файлов и каталогов, независящих от прав пользователей.
12. Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование – … угроза (ОПК-5)
активная
пассивная
13. Преднамеренная угроза безопасности информации (ОПК-5)
кража
наводнение
повреждение кабеля, по которому идет передача, в связи с погодными условиями
ошибка разработчика
14. Концепция системы защиты от информационного оружия не должна включать (ОПК-5)
средства нанесения контратаки с помощью информационного оружия;
механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры;
признаки, сигнализирующие о возможном нападении;
процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей.

Тесты к разделу 7

1. Какова конечная цель идентификации и установления подлинности объекта в вычислительной системе? (ОПК-5)
Выберите один ответ:
получение документа, сформированного непосредственно данной вычислительной системой и на аппаратуре ее документирования;
установление подлинности полученной информации;
допуск его к информации ограниченного пользования в случае положительного исхода проверки или отказ в допуске в случае отрицательного исхода проверки
2. В чем заключается разграничение доступа в вычислительной системе? (ОПК-5)
Выберите один ответ:
в перекрытии на период эксплуатации всех нештатных и технологических подходов к аппаратуре;

в создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям;
в разделении информации, циркулирующей в ней, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.
3. В чем заключается установление подлинности (аутентификация)? (ОПК-5)
Выберите один ответ:
в проверке, является ли проверяемый объект (субъект) в самом деле тем, за кого себя выдает;
в присвоении какому-либо объекту или субъекту уникального образа, имени или числа;
в получении документа, сформированного непосредственно данной вычислительной системой и на аппаратуре ее документирования.
4. Какой общеметодологический принцип предполагает, что все процедуры автоматизированной обработки защищаемой информации должны контролироваться системой защиты в полном объеме, причем основные результаты контроля должны фиксироваться в специальных регистрационных журналах? (ОПК-5)
Выберите один ответ:
активность реагирования;
экономичность СЗИ;
полнота контроля
5. Что обозначает такой общеметодологический принцип, как концептуальное единство? (ОПК-5)
Выберите один ответ:
такое построение и такую организацию функционирования, при которых функции защиты осуществлялись бы достаточно эффективно при изменении в некотором диапазоне структуры объекта обработки информации, технологических схем или условий функционирования каких-либо ее компонентов;
то, что СЗИ должна строиться в строгом соответствии с требованиями к защите, которые, в свою очередь, определяются категорией соответствующего объекта и значениями параметров, влияющих на защиту информации;
то, что архитектура, технология, организация и обеспечение функционирования как СЗИ в целом, так и составных компонентов должны рассматриваться и реализовываться в строгом соответствии с основными положениями единой концепции защиты информации.

Критерии оценки выполненных тестов:

При тестировании все верные ответы берутся за 100%.

- оценка «зачтено» выставляется обучающемуся, если тестовые задания выполнены с долей правильных ответов выше 60%

- оценка «не зачтено» выставляется обучающемуся, если тестовые задания выполнены с долей правильных ответов ниже 60%

6. Фонд оценочных средств промежуточной аттестации по дисциплине:

По итогам 1 семестра проводится зачет с оценкой. При подготовке к сдаче зачета рекомендуется пользоваться материалами практических занятий и материалами, изученными в ходе текущей самостоятельной работы.

Зачет проводится в устной или письменной форме, включает подготовку и ответы студента на теоретические вопросы.

К зачету допускаются студенты, имеющие положительные результаты по защите практических работ.

Перечень вопросов к зачету с оценкой:

1. Предмет и задачи дисциплины «Защищенные информационные системы и среды».
2. Основные задачи защиты информации.
3. Основные этапы защищенной инфраструктуры.
4. Положение о конфиденциальной информации в электронном виде.
5. Классификация информации по уровню конфиденциальности. Реквизиты документов. Хранение информации.
6. Способы хранения конфиденциальной информации. Сводная информация. Интеллектуальная собственность. Неструктурированная информация. Локальные копии
7. Основные направления защиты. Защита документов. Защита каналов утечки.
8. Мониторинг (аудит) действий пользователей.
9. Классификация внутренних нарушителей. Неосторожные. Манипулируемые. Саботажники. Нелояльные. Нарушители, мотивированные извне. Другие типы нарушителей
10. Нетехнические меры защиты от внутренних угроз. Психологические меры. Организационные меры.
11. Права локальных пользователей. Стандартизация ПО. Специфические решения.
12. Классификация firewall'oB.
13. Пакетные фильтры. Пограничные роутеры.
14. Персональные firewall'bi и персональные устройства firewall'a.
15. Прокси-сервер прикладного уровня. Выделенные прокси-серверы.
16. Гибридные технологии firewall'a. Трансляция сетевых адресов (NAT). Статическая трансляция сетевых адресов. Скрытая трансляция сетевых адресов.
17. Принципы построения окружения firewaH'a. DMZ-сети. Конфигурация с одной DMZ-сетью. Service Leg конфигурация. Конфигурация с двумя DMZ-

сетями.

18. Виртуальные частные сети.

19. Расположение VPN-серверов. Интранет. Экстранет. Компоненты инфраструктуры: концентраторы и коммутаторы. Расположение серверов в DMZ-сетях.

20. Внешне доступные серверы. VPN и Dial-in серверы. Внутренние серверы. DNS-серверы.

21. SMTP-серверы. Политика безопасности firewall'a. Политика firewall'a. Реализация набора правил firewall'a. Тестирование политики firewall'a. Возможные подходы к эксплуатации firewaH'a.

22. Сопровождение firewall'a и управление firewall'oM. Физическая безопасность окружения firewaH'a. Администрирование firewaH'a.

23. Встраивание firewall'oB в ОС.Стратегии восстановления после сбоев firewall'a.

24. Инциденты безопасности. Создание Ьаскир'ов firewall'oB

25. Основные характеристики пакетных фильтров в ОС FreeBSD.

26. ПО пакетных фильтров. OpenBSD Packet Filter (PF) и ALTQ.

27. Трансляция сетевых адресов для очень больших LAN. Использование пула публичных адресов. Port Redirection

28. Понятие системы обнаружения атак. Почему следует использовать IDS. Типы IDS.

29. Базовая архитектура IDS. Совместное расположение Host и Target. Разделение Host и Target.

30. Способы управления IDS. Централизованное управление. Частично распределенное управление. Полностью распределенное управление.

31. Скорость реакции. Информационные источники. Network-Based IDS. Host-Based IDS. Application-Based IDS.

32. Анализ, выполняемый IDS. Определение злоупотреблений. Определение аномалий. Возможные ответные действия IDS. Активные действия. Сбор дополнительной информации.

33. Изменение окружения. Выполнение действия против атакующего. Пассивные действия. Тревоги и оповещения. Использование SNMP Traps. Возможности отчетов и архивирования.

34. Системы анализа и оценки уязвимостей. Процесс анализа уязвимостей. Классификация инструментальных средств анализа уязвимостей.

35. Host-Based анализ уязвимостей.

36. Network-Based анализ уязвимостей.

37. Преимущества и недостатки систем анализа уязвимостей.

38. Системы Honey Pot и Padded Cell. Выбор IDS. Определение окружения IDS.

39. Цели и задачи использования IDS.

40. Ограничения на ресурсы, существующие в организации. Возможности IDS.

41. Развертывание IDS. Стратегия развертывания IDS.

42. Типичные выходные данные IDS.

43. Типы компьютерных атак, обычно определяемые IDS.

44. Безопасность DNS. Сервисы DNS. Инфраструктура DNS.

45. Компоненты DNS и понятие безопасности для них.

46. Основные механизмы безопасности для сервисов DNS.

47. Данные DNS и ПО DNS. Зонный файл. Name-серверы. Авторитетные name-серверы. Кэширующие name-серверы. Resolver'bi. Транзакции DNS. Запрос / ответ DNS.

48. Безопасность окружения DNS. Угрозы и обеспечение защиты платформы хоста. Угрозы ПО DNS. Угрозы для данных DNS.

49. Причины уязвимости web-сервера. Планирование развертывания web-сервера. Безопасность лежащей в основе ОС.

50. Безопасное инсталлирование и конфигурирование ОС. Применение Patch и Upgrade ОС. Удаление или запрещение ненужных сервисов и приложений. Конфигурирование аутентификации пользователя в ОС.

51. Управление ресурсами на уровне ОС. Альтернативные платформы для web-сервера. Trusted ОС.

52. Использование Appliances для web-сервера. Специально усиленные (pre-hardened) ОС и web-серверы.

53. Тестирование безопасности операционной системы. Список действий для обеспечения безопасности ОС, на которой выполняется web-сервер.

54. Безопасное инсталлирование и конфигурирование web-сервера. Безопасное инсталлирование web-сервера. Конфигурирование управления доступом.

55. Разграничение доступа для ПО web-сервера. Управление доступом к директории содержимого web-сервера.

56. Управление влиянием web Bots. Использование программ проверки целостности файлов. Список действий для безопасного инсталлирования и конфигурирования web-сервера

57. Опубликование информации на web-сайтах. Обеспечение безопасности технологий создания активного содержимого. URLs и cookies.

58. Уязвимости технологий активного содержимого на стороне клиента.

59. Уязвимости технологий создания содержимого на стороне сервера. Список действий для обеспечения безопасности web-содержимого

60. Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе. Basic-аутентификация. Digest-аутентификация.

61. SSL/TLS. Возможности SSL/TLS. Слабые места SSL/TLS. Пример SSL/TLS-сессии. Схемы шифрования SSL/TLS.Требования к реализации SSL/TLS.

62. Список действий для технологий аутентификации и шифрования. Firewall прикладного уровня для web — ModSecurity. Взаимодействие ModSecurity с пакетным фильтром

63. Демилитаризованная зона. Хостинг во внешней организации. Сетевые элементы.

64. Роутер и firewall.

65. Автоматизированные инструментальные средства анализа лог-файлов. Процедуры создания backup web-сервера.

66. Политики и стратегии выполнения backup'a web-сервера. Поддержка тестового web-сервера.

67. Поддержка аутентичной копии web-содержимого. Восстановление при компрометации безопасности.

68. Тестирование безопасности web-серверов. Сканирование уязвимостей. Тестирование проникновения.

69. Удаленное администрирование web-сервера. Список действий для безопасного администрирования web-сервера

Критерии оценки:

Ответ студента на зачете оценивается одной из следующих оценок: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», которые выставляются по следующим критериям

- *оценка «отлично» выставляется студенту, если:*

- даны исчерпывающие и обоснованные ответы на все поставленные вопросы, правильно;
- 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;

- *оценка «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.

- *оценка «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.

- *оценка «неудовлетворительно»:*

- не выполнены требования, предъявляемые к знаниям, оцениваемым “удовлетворительно”.

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. Инструментальный контроль и защита информации [Электронный ресурс]: учебное пособие/ Н.А. Свинарев [и др.].— Электрон. текстовые данные.— Воронеж: Воронежский государственный университет инженерных технологий, 2013.— 192 с.— Режим доступа: http://www.iprbookshop.ru/47422.— ЭБС «IPRbooks», по паролю
3. Метелица, Н.Т. Вычислительные сети и защита информации [Электронный ресурс]: учебное пособие/ Метелица Н.Т.— Электрон. текстовые данные.— Краснодар: Южный институт менеджмента, 2013.— 48 с.— Режим доступа: http://www.iprbookshop.ru/25962.— ЭБС «IPRbooks», по паролю
4. 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

Дополнительная литература

1. Гафнер, В.В. Информационная безопасность [Текст]: учеб. пособие/ В.В. Гафнер.– Ростов н/Д.: Феникс, 2010.
2. Корнеев, И.К. Защита информации в офисе [Текст]: учебник/ И.К. Корнеев, Е.А. Степанов.

Интернет-ресурсы

1. 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.

БОСТАНОВА ЛАУРА КЕМАЛОВНА
РЯДЧЕНКО ВИКТОР ПЕТРОВИЧ

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ И СРЕДЫ

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

Печатается в редакции авторов
Корректор
Редактор
Сдано в набор
Формат 60x84/16
Бумага офсетная.
Печать офсетная.
Усл. печ. л.
Заказ №
Тираж

Оригинал-макет подготовлен в Библиотечно-издательском центре СевКавГГТА
369000, г. Черкесск, ул. Ставропольская, 36