Бостанова Л.К.
Рядченко В.П.

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Учебно-методическое пособие для магистрантов 2 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

Бостанова Л.К.
Рядченко В.П.

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Учебно-методическое пособие для магистрантов 2 курса направления подготовки 09.04.03 Прикладная информатика

Черкесск, 2016

УДК 004.05
ББК 32.97
Б-75

Рассмотрено на заседании кафедры информатики и ИТ
Протокол № 6 от «22» декабря 2015 г.
Рекомендовано к изданию редакционно-издательским советом СевКавГГТА.
Протокол № от « 12» января 2016 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. Методы и средства обеспечения безопасности информационных систем: учебно-методическое пособие для магистрантов 2 курса направления подготовки 09.04.03 Прикладная информатика / Л.К. Бостанова, В.П. Рядченко – Черкесск: БИЦ СевКавГГТА, 2016. – 2 п.л.

В учебно-методическом пособии сформированы рекомендации для усвоения магистрантами учебного материала по курсу «Методы и средства обеспечения безопасности информационных систем», 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 «Методы и средства обеспечения безопасности информационных систем» направлен на освоение магистрантами основных понятий 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, тестовые задания.

1. Цели и задачи изучения дисциплины

Целями освоения дисциплины «Методы и средства обеспечения безопасности информационных систем» является формирование у студентов фундаментальных знаний 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 «Методы и средства обеспечения безопасности информационных систем» относится к вариативной части Блока 1 дисциплины по выбору студента (модули) (Б1.В.ДВ.5.2), 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-6	способность к профессиональной эксплуатации современного электронного оборудования в соответствии с целями основной образовательной программы магистратуры	**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-11	способность применять современные методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС	**Знать:** методы и средства обеспечения защиты информации. **Уметь:** предотвращать нарушения сетевой безопасности с использованием различных программных и аппаратных средств защиты; оценивать защищенность информационных систем. **Владеть:** методами и средствами формирования требований по защите информации, обеспечения безопасности ИС.
3.	ПК-12	способность проектировать архитектуру и сервис ИС предприятий и организаций в прикладной области	**Знать:** модели и процессы жизненного цикла, стадии и этапы проектирования ИС; технологии проектирования ИС, сервис ИС предприятий и организаций. **Уметь:** выявлять информационные потребности и разрабатывать требования к ИС; проектировать архитектуру и сервис ИС предприятий и организаций, выбирать инструментальные средства и технологии проектирования ИС; использовать международные информационные ресурсы и стандарты в информатизации предприятий и организаций. **Владеть:** методами и средствами выявления угроз безопасности

			автоматизированным системам; навыками организации и обеспечения режима секретности; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации.

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 **Системы аппаратной и программной криптографической защиты**.

Угрозы безопасности информации, АС и субъектов информационных отношений, источники угроз безопасности, классификация угроз безопасности, основные преднамеренные и непреднамеренные искусственные 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**.** Инструментальный контроль и защита информации [Электронный ресурс]: учебное пособие/ Н.А. Свинарев [и др.].— Электрон. текстовые данные.— Воронеж: Воронежский государственный университет ин-женерных

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. тек-стовые данные.— Краснодар: Южный институт менеджмента, 2013.— 48 с.— Режим доступа: http://www.iprbookshop.ru/25962.— ЭБС «IPRbooks», по паролю

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

Дополнительная литература:

1. Аверченков, В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю

2. 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

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

Тема 2. Средства стенографической и криптографической защиты информации.

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**.** Инструментальный контроль и защита информации [Электронный ре-сурс]: учебное пособие/ Н.А. Свинарев [и др.].— Электрон. текстовые данные.— Воронеж: Воронежский государственный университет ин-женерных 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. тек-стовые данные.— Краснодар: Южный институт менеджмента, 2013.— 48 с.— Режим доступа: http://www.iprbookshop.ru/25962.— ЭБС «IPRbooks», по паролю

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

Дополнительная литература:

1. Аверченков, В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю

2. 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

3. 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**.** Инструментальный контроль и защита информации [Электронный ре-сурс]: учебное пособие/ Н.А. Свинарев [и др.].— Электрон. текстовые данные.— Воронеж: Воронежский государственный университет ин-женерных технологий, 2013.— 192 с.— Режим доступа: http://www.iprbookshop.ru/47422.— ЭБС «IPRbooks», по паролю

3. Метелица, Н.Т. Вычислительные сети и защита информации [Элек-тронный ресурс]: учебное пособие/ Метелица Н.Т.— Электрон. тек-стовые данные.— Краснодар: Южный институт менеджмента, 2013.— 48 с.— Режим доступа: http://www.iprbookshop.ru/25962.— ЭБС «IPRbooks», по паролю

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

Дополнительная литература:

1. Аверченков, В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю

2. 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

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

Тема 4. Основные защитные механизмы операционной системы семейства ОС Unix и ОС Windows.

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 ОС Unix и ОС Windows.

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 ин-женерных 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. тек-стовые данные.— Краснодар: Южный институт менеджмента, 2013.— 48 с.— Режим доступа: http://www.iprbookshop.ru/25962.— ЭБС «IPRbooks», по паролю

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

Дополнительная литература:

1. Аверченков, В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон.

текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю

2. 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

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

Тема 5. Защита файлов, контроль доступа, уязвимость паролей.

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. Встраиваемые водяные знаки. DRM.

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 ин-женерных 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. тек-стовые данные.— Краснодар: Южный институт менеджмента, 2013.— 48 с.— Режим доступа: http://www.iprbookshop.ru/25962.— ЭБС «IPRbooks», по паролю

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

Дополнительная литература:

1. Аверченков, В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю

2. 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

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

Тема 6. Windows и Unix

Параметры безопасности. Настройка операционной системы. 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**.** Инструментальный контроль и защита информации [Электронный ресурс]: учебное пособие/ Н.А. Свинарев [и др.].— Электрон. текстовые данные.— Воронеж: Воронежский государственный университет ин-женерных 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. тек-стовые данные.— Краснодар: Южный институт менеджмента, 2013.— 48 с.— Режим доступа: http://www.iprbookshop.ru/25962.— ЭБС «IPRbooks», по паролю

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

Дополнительная литература:

1. Аверченков, В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю

2. 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

3. 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

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. Инструментальный контроль и защита информации [Электронный ресурс]: учебное пособие/ Н.А. Свинарев [и др.].— Электрон. текстовые данные.— Воронеж: Воронежский государственный университет ин-женерных 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. тек-стовые данные.— Краснодар: Южный институт менеджмента, 2013.— 48 с.— Режим доступа: http://www.iprbookshop.ru/25962.— ЭБС «IPRbooks», по паролю

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

Дополнительная литература:

1. Аверченков, В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю

2. 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

3. 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 данных. Обзор программ Страж NT, Secret Net .

Цель занятия: Ознакомление с основными каналами утечки информации

Вопросы для обсуждения:

1. Сканирование уязвимостей. Тестирование проникновения.
2. Программы Страж NT, Secret Net .

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 ин-женерных 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. тек-стовые

данные.— Краснодар: Южный институт менеджмента, 2013.— 48 с.— Режим доступа: http://www.iprbookshop.ru/25962.— ЭБС «IPRbooks», по паролю

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

Дополнительная литература:

1. Аверченков, В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю

2. 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

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

Практическое занятие № 2.

Тема 2. Особенности работы программ Аккорд-АМДЗ 5.5, Электронный замок «Соболь»

Цель занятия: Изучение программ Аккорд-АМДЗ 5.5, Электронный замок «Соболь»

Вопросы для обсуждения:

1. Применение Аккорд-АМДЗ 5.5.
2. Применение Электронный замок «Соболь»

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 ре-сурс]: учебное пособие/ Н.А. Свинарев [и др.].— Электрон. текстовые данные.— Воронеж: Воронежский государственный университет ин-женерных технологий, 2013.— 192 с.— Режим доступа: http://www.iprbookshop.ru/47422.— ЭБС «IPRbooks», по паролю

3. Метелица, Н.Т. Вычислительные сети и защита информации [Элек-тронный ресурс]: учебное пособие/ Метелица Н.Т.— Электрон. тек-стовые данные.— Краснодар: Южный институт менеджмента, 2013.— 48 с.— Режим доступа: http://www.iprbookshop.ru/25962.— ЭБС «IPRbooks», по паролю

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

Дополнительная литература:

1. Аверченков, В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю

2. 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

3. 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. Инструментальный контроль и защита информации [Электронный ре-сурс]: учебное пособие/ Н.А. Свинарев [и др.].— Электрон. текстовые данные.— Воронеж: Воронежский государственный университет ин-женерных технологий, 2013.— 192 с.— Режим доступа: http://www.iprbookshop.ru/47422.— ЭБС «IPRbooks», по паролю

3. Метелица, Н.Т. Вычислительные сети и защита информации [Элек-тронный ресурс]: учебное пособие/ Метелица Н.Т.— Электрон. тек-стовые данные.— Краснодар: Южный институт менеджмента, 2013.— 48 с.— Режим доступа: http://www.iprbookshop.ru/25962.— ЭБС «IPRbooks», по паролю

4. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ Прохорова О.В.— Электрон. тексто-вые данные.— Самара: Самарский государственный архитектурно-строительный

университет, ЭБС АСВ, 2014.— 113 с.— Режим досту-па: http://www.iprbookshop.ru/43183.— ЭБС «IPRbooks», по паролю

Дополнительная литература:

1. Аверченков, В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю

2. 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

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

Практическое занятие № 4.
Тема 4. Средства для защиты объектов ВТ

Цель занятия: Изучение средств для защиты объектов ВТ.
Вопросы для обсуждения:

1. Средства для обеспечения защиты объектов ВТ.
2. Средства для защиты объектов ВТ от утечки 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. Инструментальный контроль и защита информации [Электронный ре-сурс]: учебное пособие/ Н.А. Свинарев [и др.].— Электрон. текстовые данные.— Воронеж: Воронежский государственный университет ин-женерных технологий, 2013.— 192 с.— Режим доступа: http://www.iprbookshop.ru/47422.— ЭБС «IPRbooks», по паролю

3. Метелица, Н.Т. Вычислительные сети и защита информации [Элек-тронный ресурс]: учебное пособие/ Метелица Н.Т.— Электрон. тек-стовые данные.— Краснодар: Южный институт менеджмента, 2013.— 48 с.— Режим доступа: http://www.iprbookshop.ru/25962.— ЭБС «IPRbooks», по паролю

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

Дополнительная литература:

1. Аверченков, В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон.

текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 c.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю

2. 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 c.— Режим доступа: http://www.iprbookshop.ru/10677.— ЭБС «IPRbooks», по паролю

3. 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 «Методы и средства обеспечения безопасности информационных систем»

1. Виды умышленных угроз безопасности информации
2. Методы и средства защиты информации
3. Криптографические методы защиты информации
4. Secret Disc
5. Электронный ключ eToken
6. Secret Net 5.0.
7. Аккорд-АМДЗ 5.5
8. Электронный замок «Соболь»
9. Страж NT 2.5
10. Общая характеристика объектов защиты информационной деятельности и обеспечения ИБ
11. Механизм выработки детальных предложений по формированию политики и построению системы информационной безопасности.
12. Обобщенная модель способов несанкционированного доступа к источникам конфиденциальной информации.

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 реферата;
- 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

«Методы и средства обеспечения безопасности информационных систем»

Тесты к разделу 1

1. Кем защищаются национальная безопасность и законодательные данные (при этом используются передовые средства защиты информации, некоторые из которых не доступны широкой общественности)? (ОПК-6)
Выберите один ответ:
правительством
корпорациями
частными лицами
общественными организациями
2. Что из перечисленного не относится к возможным угрозам информацион-ной безопасности? (ОПК-6)
Выберите один ответ:
компьютерные преступления на основе ложной идентификации клиента
подделка электронных документов
получение злоумышленником конфиденциальной информации
кажущаяся анонимность при работе в Internet
3. Как можно определить систему защиты информации? (ПК-11)
Выберите один ответ:
как организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внеш-них угроз
как совокупность информационной инфраструктуры, субъектов, осуществ-ляющих сбор,
формирование, распространение и использование информации, а также сис-темы регулирования возникающих при этом общественных отношений
как одно из наиболее общих понятий науки, обозначающее некоторые сведе-ния, совокупность каких-либо данных, знаний и т. п.
4. Что может быть представлено как совокупность набора передаваемых све-дений и порядка (алгоритмов) их кодирования в набор знаков сообщения и декодирования в сведения? (ПК-11)
Выберите один ответ:
предложение
сообщение
сведение

5. Что составляет существо общего закона обращения информации? (ОПК-6)
Выберите один ответ:
преобразование информации из сведений в сообщения и из сообщений в сведения
возможность обмениваться с технической системой сообщениями
способность получать, накапливать и использовать для обеспечения жизнедеятельности информацию в форме сведений
6. Какой вид собственного обеспечения системы защиты информации предполагает широкое использование технических средств как для защиты информации, так и для обеспечения деятельности собственно средств защиты информации? (ПК-12)
Выберите один ответ:
лингвистическое обеспечение
организационное обеспечение
аппаратное обеспечение
7. Какой вид собственного обеспечения системы защиты информации включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы? (ПК-12)
Выберите один ответ:
аппаратное обеспечение
организационное обеспечение
информационное обеспечение
правовое обеспечение

Тесты к разделу 2

8. Какое свойство информации в форме сообщения предполагает возмож-ность количественной оценки параметров сообщения (количество знаков, составляющих сообщение)? (ОПК-6)
Выберите один ответ:
проблемная ориентированность
сложность
материальность
измеримость

9. Какой вид собственного обеспечения системы защиты информации предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты? (ПК-11)
Выберите один ответ:
нормативно-методическое обеспечение
лингвистическое обеспечение
математическое обеспечение
10.Какая причина уязвимости Интернет сформулирована неверно? (ОПК-6)
Выберите один ответ:

простота конфигурирования средств защиты
кажущаяся анонимность при работе в Internet
человеческий фактор
11. Какая причина уязвимости Интернет сформулирована неверно? (ОПК-6)
Выберите один ответ:
внедрение различными компаниями собственного дизайна при создании Web-страниц и распространение рекламной информации о своей продукции;
переизбыток организаций, занимающихся подготовкой профессионалов по защите в Internet ;
работа в Internet основана на модели клиент/сервер, не лишенной определенных слабостей и конкретных лазеек в продуктах различных производителей.
12. Кем защищаются пути доступа, малый бизнес и образовательные учреждения (при этом используются средства защиты информации среднего уров-ня, как коммерческие, так и свободно распространяемые в исследовательских центрах)? (ПК-11)
Выберите один ответ:
правительством
частными лицами
общественными организациями
корпорациями
13. Что такое безопасность информации? (ОПК-6)

Выберите один ответ:

создание компьютерных вирусов, в качестве которых выступают специально; разработанные программы, начинающие работать только по определенному сигналу;

познание окружающего мира, включающее формирование представлений о структуре окружающей среды;

способность системы ее обработки обеспечить в заданный промежуток времени возможность выполнения заданных требований по величине вероятно-сти наступления событий, выражающихся в утечке, модификации или утрате данных, представляющих ту или иную ценность для их владельца

14. Какой тип взломщиков интрасетей, согласно одной из классификаций компьютерных злоумышленников, отличается от других типов тем, что после входа в систему он должен найти и перенести определенную информацию на свой компьютер, что делает его задачу более сложной, чем простое проникновение? (ПК-12)

Выберите один ответ:

«луддит»

«хулиган»

«шпион»

15. Как называют компьютерных хулиганов, получающих удовольствие от того, что им удается проникнуть в чужой компьютер? (ОПК-6)

Выберите один ответ:

фракеры

крэкеры

хакеры

Тесты к разделу 3

16. Что является основным правовым документом, определяющим защищенность предприятия от внутренних и внешних угроз? (ОПК-6)

Выберите один ответ:
концепция современных информационных технологий
концепция безопасности информации
концепция информационных ресурсов

17. С какой точки зрения сообщения исследуются как средство воздействия на информационную модель человека, детерминирования его поведения? (ОПК-6)

Выберите один ответ:
с семантической точки зрения
с прагматической точки зрения
с технической точки зрения

18. Какая причина уязвимости Интернет сформулирована неверно? (ПК-12)

Выберите один ответ:
работа в Internet обслуживается большим числом сервисов, информационных служб и сетевых протоколов, знание правильности и тонкостей использования всех или хотя бы большинства сервисов, служб и протоколов одному человеку в лице администратора сети нереально;

«утечка» технологий высокого уровня из секретных источников при вскрытии представленных в сети Web-узлов и сетей организаций, занимающихся разработкой этих технологий, и доступность информации о средствах защиты;
зашифрованность большей части передаваемой через Internet информации

19. Как называется приверженец электронного журнала Phrack, который с 1985 г. публикует материалы по ОС, сетевым технологиям и новости компьютерного андеграунда? (ПК-12)

Выберите один ответ:
фракер
хакер
крэкер

20. Какая информация существует независимо от наличия субъекта, в рамках современных представлений точной науки непосредственно не воспринимается? (ОПК-6)

Выберите один ответ:
информация воздействия
информация взаимодействия
автономная информация

21. Какое свойство информации, поступающей к человеку в форме сведений, характеризуется возможностью изменения ценности имеющихся сведений и знаний под воздействием времени, других поступающих сведений? (ОПК-6)
Выберите один ответ:
информационная неуничтожаемостъ
субъективность
идеальность
накапливаемость
динамичность
22. Типичным примером действий какого типа взломщиков интрасетей, согласно одной из классификаций компьютерных злоумышленников, является написание и запуск компьютерных вирусных программ, например, так называемых «червей», которые плодятся в многозадачных системах и загружают процессор бесполезной работой? (ПК-12)
Выберите один ответ:
«луддита»
«шпиона»
«хулигана»

23. Как в философской литературе раскрывается понятие информации? (ОПК-6)
Выберите один ответ:
как кодированный эквивалент события, зафиксированный источником информации и выраженный с помощью последовательности условных физических символов (алфавита), образующих некоторую упорядоченную совокупность;
как одно из наиболее общих понятий науки, обозначающее некоторые сведения, совокупность каких-либо данных, знаний и т. п.;
как совокупность информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.
24. Как называют воров-взломщиков, которые воруют информацию с помощью компьютера, выкачивая целые информационные банки данных? (ПК-12)
Выберите один ответ:

фракеры

хакеры

крэкеры

25. Какая причина уязвимости Интернет сформулирована неверно? (ПК-12)
Выберите один ответ:
небольшая протяженность линий связи;

уязвимость основных служб: базовым протоколом Internet является набор протоколов TCP/IP, сервисные программы которого не гарантируют безопасности;
дизайн Internet как открытой и децентрализованной сети с изначальным отсутствием политики безопасности.

Тесты к разделу 4

26. Целью какого организационного мероприятия является исключение возможности тайного проникновения на территорию и в помещения посторонних лиц и обеспечение удобства контроля прохода и перемещения сотрудников и посетителей? (ПК-11)
Выберите один ответ:
организации работы по анализу внутренних и внешних угроз
организации работы с документами
организации работы с сотрудниками
организации использования технических средств
организации режима и охраны

27. Содержание какой функции системы защиты информации направлено на непрерывный контроль средств, комплексов, систем обработки, защиты информации и различных компонентов защищаемой информации с целью своевременного обнаружения фактов воздействия на них угроз? (ПК-11)
Выберите один ответ:
функция 1 - предупреждение проявления угроз
функция 2 - обнаружение проявившихся угроз и предупреждение их воздействия на информацию
функция 4 - ликвидация последствий воздействия угроз
функция 3 - обнаружение воздействия угроз на защищаемую информацию и локализация этого воздействия

28. Как называется одно из новых для нас направлений правовой защиты, предназначенное для защиты собственника информации и средств ее обработки как от традиционных угроз (кражи, стихийные бедствия), так и от угроз, возникающих в ходе работы с информацией? (ПК-11)
Выберите один ответ:
страховое обеспечение
правовая охрана
информационная безопасность

29. Что из перечисленного не включает в себя организационная защита? (ОПК-6)
Выберите один ответ:
организацию работы с сотрудниками
организацию использования технических средств
организацию режима и охраны
организацию разработки инструкции о порядке допуска сотрудников к сведениям, составляющим конфиденциальную информацию
организацию работы с документами

30. Как называется документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации? (ОПК-6)
Выберите один ответ:
недоступная информация
тайная информация
конфиденциальная информация
31. Согласно каким методам шифрования информации, шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите? (ПК-12)
Выберите один ответ:
аддитивным методам
методам перестановки
методам замены (подстановки)
32. Что такое организационная защита? (ОПК-6)
Выберите один ответ:
совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определенных сфер жизни и деятельности государственных органов, предприятий (организаций) и населения (отдельной личности);
регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз;
гражданское правоотношение, в силу которого одна сторона (должник) обязана совершить в пользу другой стороны определенные действия.
33. Как называется разрешение, выдаваемое государством на проведение некоторых видов хозяйственной деятельности, включая внешнеторговые операции (ввоз и вывоз) и предоставление права использовать защищенные патентами изобретения, технологии, методики? (ПК-12)
Выберите один ответ:
лицензия
договор
патент
34. Что понимается под функцией защиты? (ОПК-6)
Выберите один ответ:
множество действий, реализаций, проведение функционально однородных мероприятий, осуществляемых на объектах обработки конфиденциальной информации различными средствами, способами и методами с целью обеспечения заданных уровней защищенности информации;
однородное в функциональном отношении множество задач, обеспечивающих полную или частичную реализацию одной или нескольких целей;
организованные возможности средств, методов и мероприятий, используемых на объекте обработки информации с целью осуществления защиты

35. Как называется форма обращения со сведениями, составляющими коммерческую тайну, на основе организационных мероприятий, исключающих неправомерное овладение такими сведениями? (ОПК-6)
Выберите один ответ:
обязательство
договор
конфиденциальность

Тесты к разделу 6

36. Как называется поиск вирусов по запросу пользователя? (ОПК-6)
Выберите один ответ:
ложное срабатывание (Falsepositive)
обратный термин (Falsenegative)
сканирование по запросу (on-demand)
сканирование на лету (real-time, on-the-fly)
37. Как регулируется правовая защита на государственном уровне? (ОПК-6)
Выберите один ответ:
конвенциями
государственными и ведомственными актами
межгосударственными договорами
декларациями
38. Какие компьютерные вирусы заражают файлы-документы и электронные таблицы нескольких популярных редакторов? (ОПК-6)
Выберите один ответ:
файловые вирусы
загрузочные вирусы
сетевые вирусы
макровирусы
39. Как называется однородное в функциональном отношении множество задач, обеспечивающих полную или частичную реализацию одной или нескольких целей? (ПК-11)
Выберите один ответ:
множество функций событий
уровень событий
класс задач
40. Что из перечисленного не относится к особенностям алгоритма работы вирусов? (ОПК-6)
Выберите один ответ:
самошифрование и полиморфичность
использование нестандартных приемов
резидентность
использование «стелс»-алгоритмов
опасность
41. Что такое право? (ОПК-6)

Выберите один ответ:
совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определенных сфер жизни и деятельности государственных органов, предприятий (организаций) и населения (отдельной личности);
правовая защита информации;
разрешение, выдаваемое государством на проведение некоторых видов хозяйственной деятельности, включая внешнеторговые операции (ввоз и вывоз) и предоставление права использовать защищенные патентами изобретения, технологии, методики
42. Как называется детектирование вируса в незараженном объекте (файле, секторе или системной памяти)? (ОПК-6)
Выберите один ответ:
сканирование по запросу (on-demand)
обратный термин (Falsenegative)
сканирование на лету (real-time, on-the-fly)
ложное срабатывание (Falsepositive)
43. Какой Закон РФ определяет основы защиты информации в системах обработки и при ее использовании с учетом категорий доступа к открытой информации и к информации с ограниченным доступом? (ОПК-6)
Выберите один ответ:
Закон «Об информации, информатизации и защите информации»
Закон «Об органах государственной безопасности»
Закон «О государственной тайне»
44. Какое организационное мероприятие предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.? (ОПК-6)
Выберите один ответ:
организация режима и охраны
организация работы с документами
организация использования технических средств
организация работы с сотрудниками
организация работы по анализу внутренних и внешних угроз
45. Реализация какой функции системы защиты информации носит упреждающую цель и должна способствовать такому архитектурно-функциональному построению современных систем обработки и защиты информации, которое обеспечивало бы минимальные возможности появления дестабилизирующих факторов в различных условиях функционирования систем? (ПК-12)
Выберите один ответ:
функция 2 - обнаружение проявившихся угроз и предупреждение их воздействия на информацию

функция 4 - ликвидация последствий воздействия угроз
функция 3 - обнаружение воздействия угроз на защищаемую информацию и локализация этого воздействия
функция 1 - предупреждение проявления угроз
46. К каким задачам защиты информации относится класс 1.2. «Дезинформация противника»? (ОПК-6)
Выберите один ответ:
к задачам уменьшения степени распознавания объектов
к задачам защиты информации от информационного воздействии
к задачам защиты содержания обрабатываемой, хранимой и передаваемой информации
47. Что на сегодняшний день является основным источником вирусов? (ОПК-6)
Выберите один ответ:
пиратское программное обеспечение
ремонтные службы
глобальная сеть Internet
персональные компьютеры общего пользования
48. В алгоритм каких вирусов заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти и др. (по классификации компьютерных вирусов по деструктивным возможностям)? (ПК-11)
Выберите один ответ:
опасных вирусов
безвредных вирусов
очень опасных вирусов
неопасных вирусов

49. Какие компьютерные вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты? (ПК-12)
Выберите один ответ:
файловые вирусы
загрузочные вирусы
сетевые вирусы
макровирусы

Тесты к разделу 7

50. Что такое коммерческая тайна? (ОПК-6)
Выберите один ответ:
не являющиеся государственными секретами сведения, связанные с производством, технологией, управлением, финансами и другой деятельностью, разглашение, утечка и несанкционированный доступ к которой может нанести ущерб их владельцам
разрешение, выдаваемое государством на проведение некоторых видов хозяйственной деятельности, включая внешнеторговые операции (ввоз и вывоз)

и предоставление права использовать защищенные патентами изобретения, технологии, методики
гражданское правоотношение, в силу которого одна сторона (должник) обязана совершить в пользу другой стороны определенные действия
51. В чем заключается основная задача систем контроля вскрытия аппаратуры?
Выберите один ответ:
в разделении информации, циркулирующей в ней, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями
в перекрытии на период эксплуатации всех нештатных и технологических подходов к аппаратуре
в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы
в создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям
52. Суть каких методов шифрования информации состоит в том, что входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов?
Выберите один ответ:
аддитивных методов
методов перестановки
методов замены (подстановки)
53. Что такое система защиты информации?
Выберите один ответ:
организованная совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) на объекте обработки информации (ООИ) для решения в ней выбранных задач защиты;
организованная совокупность тех функций системы, для регулярного осуществления которых она создается;
общая организация системы, адекватно отражающая концептуальные подходы к ее созданию
54. Как называется комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей?
Выберите один ответ:
защита информации от утечки по акустическому каналу
защита информации от утечки по электромагнитным каналам
защита информации от утечки по визуально-оптическому каналу
55. В чем заключается ограничение доступа?
Выберите один ответ:

в разделении информации, циркулирующей в ней, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;
в создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям;
в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;
в перекрытии на период эксплуатации всех нештатных и технологических подходов к аппаратуре.
56. В чем заключается основная задача разделения привилегий на доступ к информации?
Выберите один ответ:
в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ;
в существенном затруднении преднамеренного перехвата информации нарушителем;
в перекрытии на период эксплуатации всех нештатных и технологических подходов к аппаратуре.
57. В каком случае может возникнуть паразитная генерация усилителей?
Выберите один ответ:
из-за напряженности суммарного поля, определяющей электромагнитную обстановку в энергетическом помещении;
из-за появления электромагнитного излучения или электрического тока;
из-за неконтролируемой положительной обратной связи за счет конструктивных особенностей схемы или за счет старения элементов.
58. Как называется комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии?
Выберите один ответ:
защита информации от утечки по визуально-оптическому каналу
защита информации от утечки по акустическому каналу
защита информации от утечки по электромагнитным каналам
59. Что такое функциональное построение СЗИ?
Выберите один ответ:
совокупность специально выделенных для обеспечения защиты информации сотрудников, выполняющих свои функции в соответствии с разработанными правилами, а также нормативная база, регламентирующая выполнение этих функций;
общая организация системы, адекватно отражающая концептуальные подходы к ее созданию;
организованная совокупность тех функций, для регулярного осуществления которых она создается.

60. В чем заключается защита информации методом криптографического преобразования?
Выберите один ответ:
в преобразовании ее составных частей (слов, букв, слогов, цифр) с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т. е. в приведении ее к неявному виду;
в определении эффективности защиты звукоизоляции;
в исключении или уменьшении возможности выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии.

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 3 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 «Методы и средства обеспечения безопасности информационных систем».
2. Основные задачи защиты информации.
3. Основные этапы защищенной инфраструктуры.
4. Классификация стеганографии
5. Классическая стеганография
6. Симпатические чернила
7. Другие стеганографические методы
8. Стеганографические модели
9. Основные понятия
10. Компьютерная стеганография
11. Цифровая стеганография
12. Сетевая стеганография.Алгоритмы
13. Метод LSB
14. Эхо-методы

15.Фазовое кодирование
16.Метод расширенного спектра
17. Атаки на стегосистемы
18.Стеганография и цифровые водяные знаки
19. Применение стеганографии
20. В современных принтерах
21. Применение цифровой стеганографии
22. Предполагаемое использование террористами
23. Предполагаемое использование спецслужбами
24. Классификация стеганографии
25.Классическая стеганография
26.Симпатические чернила
27.Другие стеганографические методы
28. Стеганографические модели
29. Основные понятия
30. Компьютерная стеганография
31.Цифровая стеганография
32.Сетевая стеганография.Алгоритмы
33.Метод LSB
34.Фазовое кодирование
35.Метод расширенного спектра
36. Атаки на стегосистемы
37.Стеганография и цифровые водяные знаки
38. Применение стеганографии
39. В современных принтерах
40. Применение цифровой стеганографии
41. Предполагаемое использование террористами
42. Предполагаемое использование спецслужбами

Критерии оценки:

Критерии оценивания:

Ответ студента на зачете оценивается одной из следующих оценок: «зачтено» и «незачтено», которые выставляются по следующим критериям

Оценка «зачтено» выставляется студенту, если:

даны исчерпывающие и обоснованные ответы на 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.

Также оценка «зачтено» выставляется студенту, если:

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.

Наконец, оценкой «зачтено» оцениваются ответы студентов если:

даны в основном правильные ответы на все поставленные вопросы, но без должной глубины и обоснования, на уточняющие вопросы даны правильные ответы; ответы были многословными, нечеткими и без должной логической последовательности; на отдельные дополнительные вопросы не даны положительные ответы.

Оценка «незачтено» выставляется студентам,

ответы, которых, носят несистематизированный, отрывочный, поверхностный характер, когда студент не понимает существа излагаемых им вопросов, что свидетельствует о том, что он не может дальше продолжать обучение или приступать к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине

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 ин-женерных 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. тек-стовые данные.— Краснодар: Южный институт менеджмента, 2013.— 48 с.— Режим доступа: http://www.iprbookshop.ru/25962.— ЭБС «IPRbooks», по паролю

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

Дополнительная литература:

1. Аверченков, В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический

университет, 2012.— 184 c.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю

2. 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 c.— Режим доступа: http://www.iprbookshop.ru/10677.— ЭБС «IPRbooks», по паролю

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

8. Учебно-методическое и информационное обеспечение дисциплины

Интернет-ресурсы

1. Электронно-библиотечная система IPRbooks URL: http://www.iprbookshop.ru/. ООО «Ай Пи Эр Медиа». Контракт №1801/16 от 01.07.2016г. на 5000 (пять тысяч) доступов.

БОСТАНОВА ЛАУРА КЕМАЛОВНА
РЯДЧЕНКО ВИКТОР ПЕТРОВИЧ

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Учебно-методическое пособие для магистрантов 2 курса направления подготовки 09.04.03 Прикладная информатика

Печатается в редакции авторов

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