МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования

«Институт сервиса, туризма и дизайна (филиал) ФГАОУ ВПО «Северо-Кавказский федеральный университет» в г. Пятигорске»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для студентов по организации самостоятельной работы

по дисциплине

Комплексная система защиты информации на предприятии

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль)	Комплексная защита объектов информатизации
Квалификация выпускника	Бакалавр
Форма обучения	Очная

Пятигорск 2020

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ 3
2. КОМПЕТЕНЦИИ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ 3
3. ТЕХНОЛОГИЧЕСКАЯ КАРТА САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТА 4
4. ТЕМЫ ДЛЯ САМОСТОЯТЕЛЬНОГО ИЗУЧЕНИЯ 5
5. ПОДГОТОВКА К ЛАБОРАТОРНЫМ ЗАНЯТИЯМ И КУРСОВОЙ РАБОТЕ 6
6. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ 10
7. КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ 11
8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 12

1. Цель и задачи освоения дисциплины

Целью освоения дисциплины «Комплексная система защиты информации на предприятии» является теоретическая и практическая подготовка студентов в области проектирования, создания и эксплуатации комплексных систем защиты информации на предприятии.

Задачи освоения дисциплины: сущность и задачи комплексной системы защиты информации (КСЗИ); принципы организации и этапы разработки КСЗИ; определение и нормативное закрепление объектов и субъектов защиты; анализ и оценка угроз безопасности информации; определение компонентов КСЗИ; построение моделей КСЗИ; принципы и методы планирования функционирования КСЗИ; состав методов и моделей оценки эффективности КСЗИ.

2. КОМПЕТЕНЦИИ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Код	Формулировка:
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
ПК-3	способностью администрировать подсистемы информационной безопасности объекта защиты
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК-7	способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
ПК-8	способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации
ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
ПК-15	способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	Изучение литературы по темам 1-9	Конспект	собеседование	4,36	0,49	4,85
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	Подготовка к лекциям	Конспект	собеседование	1,21	0,14	1,35
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	подготовка к лабораторным работам	Отчет	отчет письменный	7,29	0,81	8,1
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	подготовка к практическим занятиям	Отчет	отчет письменный	6,07	0,68	6,75
ОПК-7, ПК-1, ПК-2, ПК-3, ПК-4, ПК-7, ПК-8, ПК-12, ПК-13, ПК-15	Выполнение курсовой работы	Курсовая работа	Курсовая работа	11,43	1,27	12,7
			Итого	30,37	3,38	33.75

4. ТЕМЫ ДЛЯ САМОСТОЯТЕЛЬНОГО ИЗУЧЕНИЯ

Для успешного освоения дисциплины, необходимо выполнить следующие виды самостоятельной работы, используя рекомендуемые источники информации

Работа с литературой:

№ п/п	Виды самостоятельной работы	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая	Интернет-

			я	литература	ресурсы
1.	изучение литературы по темам 1-9	1,2	1,2	1-3	1-2
2.	проработка лекционного материала	1,2	1,2	1-3	1-2

Оценочные средства: собеседование

5. ПОДГОТОВКА К ЛАБОРАТОРНЫМ РАБОТАМ И КУРСОВОЙ РАБОТЕ

№ п/п	Виды самостоятельной работы	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая литература	Интернет-ресурсы
3.	подготовка к лабораторным работам	1,2	1,2	1-3	1-2
4.	подготовка к практическим занятиям	1,2	1,2	1-3	1-2
5.	Выполнение курсовой работы	1,2	1,2	1-4	1-2

Оценочные средства: отчёт письменный

7. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Вопросы к экзамену

Вопросы к экзамену (5 семестр)

Вопросы для проверки уровня обученности:

Знать:

1. Задачи и функции комплексной системы защиты информации на предприятии.
2. Принципы организации и этапы разработки комплексной системы защиты информации.
3. Цели создания КСЗИ на предприятии.
4. Принципы построения КСЗИ на предприятии.
5. Общее содержание работ по организации КСЗИ.
6. Классификация формальных моделей безопасности.
7. Модели обеспечения конфиденциальности информации.
8. Модели обеспечения целостности информации.
9. Субъектно-ориентированная модель безопасности информации.
10. Взаимосвязь КСЗИ с другими системами предприятия.
11. Методологические основы организации КСЗИ.
12. Принципы построения КСЗИ и взаимодействие с другими подразделениями предприятия.
13. Режим секретности на предприятии.
14. Правовая основа режима секретности на предприятии.

15. Нормативно-правовые аспекты защиты государственной тайны.
16. Нормативно-правовые аспекты защиты коммерческой тайны.
17. Факторы и угрозы безопасности информации.
18. Методика выявления нарушителей, тактики их действий и состава интересующей их информации.
19. Модели нарушителей угроз безопасности предприятия.
20. Защита от утечки информации по техническим каналам в автоматизированных системах.
21. Защита от несанкционированного доступа к информации в автоматизированных системах.
22. Организационно-распорядительные документы организации для подготовки к работе на автоматизированных системах.
23. Особенности защиты речевой информации на предприятии.
24. Условия функционирования КСЗИ на предприятии.
25. Влияние формы собственности на особенности защиты информации ограниченного доступа.
26. Влияние организационно-правовой формы предприятия на особенности защиты информации ограниченного доступа.
27. Факторы, определяющие необходимость защиты периметра здания предприятия.
28. Особенности помещений как объектов защиты для работы по защите информации.
29. Роль и место внутриобъектового и пропускного режимов в системе защиты информации предприятия.
30. Силы и средства, используемые при организации внутриобъектового режима.
31. Модели КСЗИ (принцип формализации требований безопасности и условий функционирования системы).
32. Основные подходы к проектированию КСЗИ на предприятии.
33. Кадровый аспект обеспечения безопасности информации.
34. Основные положения мероприятий по аттестации объектов информатизации.
35. Программа аттестационных испытаний автоматизированной системы.
36. Экспертно-документальный метод проведения аттестационных испытаний.
37. Сертификация средств защиты информации, использующихся при построении КСЗИ предприятия.
38. Виды контроля функционирования КСЗИ.
39. Цели проведения контрольных мероприятий в КСЗИ.

Уметь, владеть:

1. Классификация информации по видам тайн.
2. Разработка политики безопасности и регламента безопасности предприятия.
3. Система допуска должностных лиц, граждан, организаций к государственной тайне.
4. Засекречивание и рассекречивание сведений и их носителей.
5. Порядок внедрения Перечня сведений, составляющих коммерческую тайну, внесение в него изменений и дополнений.
6. Методика определения состава защищаемой информации на предприятии.
7. Методика выявления состава носителей защищаемой информации.
8. Обязанности и запреты сотрудников, допущенных к конфиденциальной информации.

9. Подходы к оценке ущерба от нарушений ИБ.
10. Реагирование на инциденты ИБ.
11. Обеспечение безопасности информации в непредвиденных ситуациях.
12. Подготовка мероприятий на случай возникновения чрезвычайных ситуаций.
13. Резервирование информации и отказоустойчивость.
14. Разработка технологического процесса автоматизированной обработки и хранения информации на предприятии.
15. Определение возможностей несанкционированного доступа к речевой информа ции, обрабатываемой во время проведения закрытых совещаний на предприятии.
16. Основные подходы и принципы к организации внутриобъектового режима.
17. Этапы разработки КСЗИ на предприятии.
18. Экономический подход к оценке эффективности комплексной системы защиты информации на предприятии.
19. Организация управления, планирование функционирования и оценка эффективности КСЗИ.
20. Методы проверок и испытаний объектов информатизации, используемые при аттестации.
21. Методики аттестационных испытаний автоматизированной системы.

8. КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Оценка «отлично» выставляется студенту, если глубокие, исчерпывающие знания и творческие способности в понимании, изложении и использовании учебно-программного материала; логически последовательные, содержательные, полные, правильные и конкретные ответы на все поставленные вопросы и дополнительные вопросы преподавателя; свободное владение основной и дополнительной литературой, рекомендованной учебной программой.

Оценка «хорошо» выставляется студенту, если твердые и достаточно полные знания всего программного материала, правильное понимание сущности и взаимосвязи рассматриваемых процессов и явлений; последовательные, правильные, конкретные ответы на поставленные вопросы при свободном устранении замечаний по отдельным вопросам; достаточное владение литературой, рекомендованной учебной программой.

Оценка «удовлетворительно» выставляется студенту, если твердые знания и понимание основного программного материала; правильные, без грубых ошибок ответы на поставленные вопросы при устранении неточностей и несущественных ошибок в освещении отдельных положений при наводящих вопросах преподавателя; недостаточное владение литературой, рекомендованной учебной программой.

Оценка «неудовлетворительно» выставляется студенту, если неправильные ответы на основные вопросы, допущены грубые ошибки в ответах, непонимание сущности излагаемых вопросов; неуверенные и неточные ответы на дополнительные вопросы.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1. Рекомендуемая литература

9.1.1. Основная литература:

1. Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации: Учебное пособие. Изд. 4-е, перераб. и доп. - М.: ЛЕНАНД, 2016. – 416 с. (Основы защиты информации. №1) ISBN 978-5-9710-2667-9
2. Будников С.А., Паршин Н.В. Информационная безопасность автоматизированных систем. Воронеж: ГУП ВО «Воронежская областная типография – издательство им. Е.А. Болховитинова». – 2011. – 354 с. ISBN 978-5-87456-944-0
3. Обеспечение информационной безопасности деятельности учебного заведения / В.А. Шевцов, В.П. Мельников, А.И. Куприянов, А.М. Петраков; под ред. проф. В.П. Мельникова. – М.: Вузовская книга, 2012. – 532 с.: ил. ISBN 978-5-9502-0531-6
4. Росенко А.П. Внутренние угрозы безопасности конфиденциальной информации: Методология и теоретическое исследование. М.: КРАСАНД, 2010. – 160 с. ISBN 978-5-396-00121-3
5. Сёмкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие. – М.: Гелиос АРВ, 2005. – 192 с. ISBN 5-85438-042-0
6. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.:ил. ISBN 978-5-91180-855-6
7. Торокин А.А. Инженерно-техническая защита информации: учебное пособие для студентов, обучающихся по специальностям в области информационной безопасности – М.: Гедиос АРВ, 2005. – 960 с: ил.. ISBN 5-85438-140-0
8. Хорев А.А. Техническая защита информации: учебное пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. – М.:НПЦ «Аналитика», 2008. – 436 с.: ил. ISBN 978-59901488-1-9
9. Язов Ю.К., Соловьев С.В. Защита информации в информационных системах от несанкционированного доступа. Пособие. – Воронеж: Кварта, 2015. – 440 с. ISBN 978-5-93737-107-2

10.1.2. Перечень дополнительной литературы:

1. Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. Изд. М.: ЛЕНАНД, 2016. – 248 с. (Основы защиты информации. №2) ISBN 978-5-9710-2737-9
2. Северин В.А. Правовая защита информации в коммерческих организциях: Учебное пособие для студентов высших учебных заведений / под ред. Б.И. Пугинского. – М.: Издательский центр «Академия», 2009. – 224 с. ISBN 978-5-7695-5563-3
3. Стандарты информационной безопасности: курс лекций: учебное пособие / Второе издание / В.А. Галатенко. Под редакцией академика РАН В.Б. Бетелина / - М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2012. – 264 с.

9.1.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине:

1. Методические рекомендации для студентов по организации и проведению самостоятельной работы по дисциплине Комплексная система защиты информации на предприятии.
2. Методические указания по выполнению лабораторных работ по дисциплине Комплексная система защиты информации на предприятии.
3. Методические указания по выполнению практических занятий по дисциплине Комплексная система защиты информации на предприятии.
4. Методические указания по выполнению курсовой работы по дисциплине Комплексная система защиты информации на предприятии.

9.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

1. http://biblioclub.ru

2. http://elibrary.ru/