МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт физики

подписано электронно-цифровой подписью

Программа дисциплины

Комплексное обеспечение информационной безопасности Б3.В.5

Направление подготовки: 090900.62 - Информационная безопасность
Профиль подготовки: Информационная безопасность автоматизированных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Ситников С.Ю.

Рецензент(ы):

Шерстюков О.Н.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Шерстюков О. Н.
Протокол заседания кафедры No ___ от "____" _____ 201__г

Учебно-методическая комиссия Института физики:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 6170214

Казань
2014

Содержание

Программу дисциплины разработал(а)(и) Ситников С.Ю. , Sergey.Sitnikov@kpfu.ru

1. Цели освоения дисциплины

развитие у студентов личностных качеств, а также формирование общекультурных-универсальных (общенаучных, социально-личностных, инструментальных) и профессиональных компетенций в соответствии с требованиями ФГОС ВПО по данному направлению подготовки формирование универсальных (общенаучных, социально-личностных, общекультурных и инструментальных) и профессиональных (общепрофессиональных и профильно-специализированных) компетенций, позволяющих выпускнику успешно работать в избранной сфере деятельности, быть социальной мобильным и устойчивым на рынке труда укрепление равственности, развитие общекультурных потребностей, творческих способностей, социальной адаптации, коммуникативности, толерантности, настойчивости в достижении цели, выносливости и физической культуре

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б3.В.5 Профессиональный" основной образовательной программы 090900.62 Информационная безопасность и относится к вариативной части. Осваивается на 4 курсе, 7 семестр.

Дисциплина предназначена для подготовки бакалавров в соответствии с требованиями направления подготовки "Радиофизика", профилем подготовки "Информационная безопасность". Для освоения дисциплины необходимы знания дисциплин: информатика, радиотехника и радиоэлектроника, физические основы информационных систем. Освоение дисциплины будет способствовать успешной профессиональной деятельности, позволит сформировать у будущих специалистов представление о современных методах решения задач, связанных с организационным обеспечением информационной безопасности, построением системы защиты объекта и практическим определением возможных каналов утечки информации на конкретном объекте.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-1 (общекультурные компетенции)	способностью осознавать необходимость соблюдения Конституции Российской Федерации, прав и обязанностей гражданина своей страны, гражданского долга и проявления патриотизма
ОК-2 (общекультурные компетенции)	способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм
ОК-5 (общекультурные компетенции)	способностью к кооперации с коллегами, работе в коллективе
ОК-6 (общекультурные компетенции)	способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-5 (профессиональные компетенции)	способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации
ПК-6 (профессиональные компетенции)	способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов
ПК-7 (профессиональные компетенции)	способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий
ПК-8 (профессиональные компетенции)	способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия

В результате освоения дисциплины студент:

1. должен знать:

Знать:

нормативно-правовые основы и документы по проблеме организационного обеспе-чения информационной безопасности, основные составляющие проблемы и концептуальные положения, угрозы информационной безопасности и меры защиты и противодей-ствия, основные мероприятия по созданию и обеспечению функционирования комплекс-ной системы защиты; требования и рекомендации по защите информации и требования по технической защите информации.

2. должен уметь:

Уметь:

использовать нормативно-правовую базу в решении задач обеспечения информаци-онной безопасности и комплексной защиты информации на предприятии и в организации; строить концептуальные модели информационной безопасности объекта, формули-ровать основные задачи по созданию и обеспечению функционирования комплексной системы защиты на предприятии, в организации.

3. должен владеть:

Владеть:

навыками работы с нормативно-правовыми и организационно-распорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутриобъектового режима.

4. должен демонстрировать способность и готовность:

Знать:

нормативно-правовые основы и документы по проблеме организационного обеспе-чения информационной безопасности, основные составляющие проблемы и концепту-альные положения, угрозы информационной безопасности и меры защиты и противодей-ствия, основные мероприятия по созданию и обеспечению функционирования комплекс-ной системы защиты; требования и рекомендации по защите информации и требования по технической защите информации.

Уметь:

использовать нормативно-правовую базу в решении задач обеспечения информаци-онной безопасности и комплексной защиты информации на предприятии и в организа-ции; строить концептуальные модели информационной безопасности объекта, формули-ровать основные задачи по созданию и обеспечению функционирования комплексной системы защиты на предприятии, в организации.

Владеть:

навыками работы с нормативно-правовыми и организационно-распорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутриобъектового режима.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы) 144 часа(ов).

Форма промежуточного контроля дисциплины экзамен в 7 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Методы, проблемы, стратегии и уровни информационной безопасности	7	1	4	0	4	устный опрос
2.	Тема 2. Концептуальные положения организационного обеспечения ИБ	7	3	4	0	4	устный опрос
3.	Тема 3. Информационная безопасность на объекте	7	5	4	0	4	устный опрос
4.	Тема 4. Конфиденциальная информация	7	7	4	0	4	устный опрос

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
5.	Тема 5. Организационная структура и основные мероприятия по созданию и обеспечению функционирования комплексной системы ЗИ	7	9	4	0	4	устный опрос
6.	Тема 6. Система организационно-распорядительных документов по организации комплексной системы ЗИ	7	11	4	0	4	устный опрос
7.	Тема 7. Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО	7	13	4	0	4	устный опрос
8.	Тема 8. Технология защиты от угроз экономической безопасности	7	15	4	0	4	устный опрос
9.	Тема 9. Требования и рекомендации по защите информации	7	17	4	0	4	устный опрос
.	Тема . Итоговая форма контроля	7		0	0	0	экзамен
	Итого			36	0	36	

4.2 Содержание дисциплины

Тема 1. Методы, проблемы, стратегии и уровни информационной безопасности

лекционное занятие (4 часа(ов)):

1.1 Задачи и методы комплексного обеспечения ИБ. Содержание основных используемых в ИБ понятий. Определение за-щиты информации. Основные методы обеспечения ИБ. 1.2 Проблема ИБ. Определение ИБ. Актуальные проблемы создания и совершенствования системы ЗИ. Эле-менты эффективной и гибкой системы управления региональной системы ЗИ и основные вопросы, решаемые при её создании. Два вида про-блем. 1.3. Основные составляющие ИБ. Категории спектра интересов, свя-занных с использованием инф. си-стем. Понятия доступности, целост-ности и конфиденциальности, их смысл в контексте проблемы ИБ.

лабораторная работа (4 часа(ов)):

Стратегия ИБ и её цели. Определение понятия. Главные цели ИБ. Административный уровень ИБ. Программа безопасности и политика безопасности. Процедурный уровень защиты. Уровни детализации политики безопасности, основные документы и их разделы.

Тема 2. Концептуальные положения организационного обеспечения ИБ

лекционное занятие (4 часа(ов)):

2.1. Общие сведения о доктрине и концепции организационного обеспе-чения безопасности. Цель и область применения концепции. Основания и исходные данные для разработки кон-цепции. 2.2. Задачи обеспечения нацио-нальной безопасности в информа-ционной сфере. Наиболее значимые задачи в гуманитарной области и в области обеспечения безопасности информационной инфраструктуры и ресурсов.

лабораторная работа (4 часа(ов)):

Методы работы с персоналом. Понятие и состав персонала, как источника информации. Основные направления сотрудничества сотрудника организации со злоумышленником. Особенности приема сотрудников на работу с информацией ограниченного доступа. Подготовительные этапы, активный и пассивный методы. Технологическая цепочка процесса приема.

Тема 3. Информационная безопасность на объекте

лекционное занятие (4 часа(ов)):

3.1 Угрозы ИБ на объекте. Источ-ники угроз безопасности. Деление источников угроз на группы, субъек-ты угроз. Виды угроз безопасности, классификация. Дополнительное де-ление на внутренние и внешние угро-зы. Каналы утечки информации. 3.2 Модель угроз безопасности на объекте. Методы защиты. Основ-ные группы методов (способов) за-щиты информации. Основные уровни защиты. 3.3 Принципы комплексной защи-ты информации. Основные принци-пы. Расшифровка понятий. 3.4 Система обеспечения ИБ, общие сведения об ИТКС. Стадии создания системы обеспечения безопасности. Организационные и технические мероприятия на каждой из стадий. Мероприятия, проводимые в процессе эксплуатации ИТКС. Понятие необходимого уровня защиты.

лабораторная работа (4 часа(ов)):

3.5. Предпосылки появления угроз в ИТКС, их возможные разновидно-сти, интерпретация. Определение угрозы ИБ в ИТКС. Существующие классификации угроз и их источни-ков в ИТКС. 3.6. Классификация угроз безопас-ности в ИТКС по 5 группам различ-ных угроз. Классификация угроз в ИТКС по источнику возможной опасности. Классификация по защите информации от НСД. Четыре уровня угроз в модели нарушителя в АСОД. Классификация угроз по способам их возможного негативного воздействия с описанием способов реализации. Критерии деления множества угроз в ИТКС на классы. Наиболее опасные угрозы ИБ в ИТКС. Воздействия нарушителя на систему на различных этапах функционирования ИТКС, направления воздействия. 3.6. Уязвимости. Причины появле-ния уязвимостей. Воздействия нару-шителя на систему через её уязвимо-сти на различных этапах функциони-рования ИТКС. Реализация угроз че-рез КНПИ. Классификация КНПИ по двум критериям.

Тема 4. Конфиденциальная информация

лекционное занятие (4 часа(ов)):

4.1. Организация службы безопас-ности объекта. Отношения объекта и субъекта в информационном про-цессе с противоположными интере-сами с позиции активности в дей-ствиях. Определение понятия утеч-ки информации. Уязвимые места в ИБ. Признаки наличия уязвимых мест. Примеры, способствующие неправомерному овладению конфи-денциальной информацией. Каналы, способы и средства. Формы и мето-ды недобросовестной конкуренции в контексте проблемы защиты ин-формации. Совокупность определе-ний, способов и средств НСД к ин-формации на объекте. 4.2. Направления обеспечения ИБ на объекте. Нормативно-правовые категории. Направления обеспечения безопасности и защиты информации. Защитные действия и их характери-стики. Средства и методы организа-ционной защиты. Определение орга-низационной защиты. Состав меро-приятий организационной защиты. 4.3. Специальные штатные служ-бы и структуры ЗИ. Служба без-опасности предприятия, её струк-турные единицы. Задачи службы безопасности предприятия. 4.4. Концепция создания физиче-ской защиты важных объектов. Основные термины и определения. Система физической защиты, опре-деление. Деление СФЗ на подсисте-мы. Стадии проектирования объек-тов защиты. Основные этапы стадии концептуального проекта. Концеп-ция физической безопасности объ-екта. Основные вопросы концепции: предметы защиты, угрозы безопас-ности и модель вероятных исполни-телей угроз, оценка и анализ уязви-мости и общие рекомендации по обеспечению безопасности объекта. Меры физической безопасности.

лабораторная работа (4 часа(ов)):

Концепция создания физиче-ской защиты важных объектов. Основные термины и определения. Система физической защиты, опре-деление. Деление СФЗ на подсисте-мы. Стадии проектирования объек-тов защиты. Основные этапы стадии концептуального проекта. Концеп-ция физической безопасности объ-екта. Основные вопросы концепции: предметы защиты, угрозы безопас-ности и модель вероятных исполни-телей угроз, оценка и анализ уязви-мости и общие рекомендации по обеспечению безопасности объекта. Меры физической безопасности.

Тема 5. Организационная структура и основные мероприятия по созданию и обеспечению функционирования комплексной системы ЗИ

лекционное занятие (4 часа(ов)):

5.1. Цели, задачи и субъекты ИБ. Основные цели и задачи обеспечения ИБ. Управление ИБ. Классификация субъектов, влияющих на состояние ИБ. 5.2. Организационная структура системы обеспечения ИБ. Регла-ментация действий пользователей и обслуживающего персонала АС. Служба (подразделение) ЗИ. Уровни организационной структуры системы обеспечения ИБ АС организации. Технология обеспечения ИБ.

лабораторная работа (4 часа(ов)):

Основные мероприятия по созданию и обеспечению функционирования комплексной системы ЗИ. Классификация мероприятий. Распределение функций по обеспечению ИБ.

Тема 6. Система организационно-распорядительных документов по организации комплексной системы ЗИ

лекционное занятие (4 часа(ов)):

6.1. Концепция обеспечения ИБ на предприятии. Документ ?Концепция обеспечения ИБ организации?.

лабораторная работа (4 часа(ов)):

Категорирование и перечень информационных ресурсов, подлежащих защите. Положение об определении требований по защите (категорировании) ресурсов. Классификация защищаемой информации. Инструкции по организации защиты.

Тема 7. Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО

лекционное занятие (4 часа(ов)):

7.1. Задачи концептуального проектирования. Концептуальный проект. Оценка эффективности вариантов. 7.2. Создание службы безопасности организации. Разрешенные виды деятельности СБ. Организация службы экономической безопасности. Этапы, рекомендуемые при создании СЭБ.

лабораторная работа (4 часа(ов)):

Структура службы экономической безопасности

Тема 8. Технология защиты от угроз экономической безопасности

лекционное занятие (4 часа(ов)):

8.1. Общий алгоритм действий и активная модель реагирования. Последовательность операций (дей-ствий). Система предупредительных мер. Нестандартные угрозы. Актив-ная модель реагирования. 8.2. Предупредительная работа с персоналом. Индикаторы выявле-ния. Потенциальные нарушители. Проверки персонала, некоторые способы.

лабораторная работа (4 часа(ов)):

Служба безопасности и проверка контрагентов. Причины, снижающие надежность контрагентов. Криминалистическая экспертиза документов. Формирование картотеки клиентов и участие организации в формировании банков данных о контрагентах.

Тема 9. Требования и рекомендации по защите информации

лекционное занятие (4 часа(ов)):

10.1. Требования по технической защите информации. Организация охраны объектов. 11.1. Организационно-пропускной режим на предприятии. 11.2. Подготовка исходных данных. 11.3. Оборудование пропускных пунктов. 11.4. Организация пропускного ре-жима. Система защиты информации и ее задачи. 12.1. Организационная система за-щиты информации. Государственная политика и об-щее руководство деятельностью по защите информации.

лабораторная работа (4 часа(ов)):

Направления формирования системы защиты информации. Этапы реализации концепции защиты информации. Финансирование мероприятий по защите информации. Результаты реализации концепции защиты информации.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Методы, проблемы, стратегии и уровни информационной безопасности	7	1	подготовка к устному опросу	4	устный опрос
2.	Тема 2. Концептуальные положения организационного обеспечения ИБ	7	3	подготовка к устному опросу	4	устный опрос
3.	Тема 3. Информационная безопасность на объекте	7	5	подготовка к устному опросу	4	устный опрос
4.	Тема 4. Конфиденциальная информация	7	7	подготовка к устному опросу	4	устный опрос
5.	Тема 5. Организационная структура и основные мероприятия по созданию и обеспечению функционирования комплексной системы ЗИ	7	9	подготовка к устному опросу	4	устный опрос
6.	Тема 6. Система организационно-распорядительных документов по организации комплексной системы ЗИ	7	11	подготовка к устному опросу	4	устный опрос
7.	Тема 7. Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО	7	13	подготовка к устному опросу	4	устный опрос

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
8.	Тема 8. Технология защиты от угроз экономической безопасности	7	15	подготовка к устному опросу	4	устный опрос
9.	Тема 9. Требования и рекомендации по защите информации	7	17	подготовка к устному опросу	4	устный опрос
	Итого				36	

5. Образовательные технологии, включая интерактивные формы обучения

лекция-визуализация, мультимедийная презентация

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Методы, проблемы, стратегии и уровни информационной безопасности

устный опрос , примерные вопросы:

1.1 Задачи и методы комплексного обеспечения ИБ. Содержание основных используемых в ИБ понятий. Определение за-щиты информации. Основные методы обеспечения ИБ. 1.2 Проблема ИБ. Определение ИБ. Актуальные проблемы создания и совершенствования системы ЗИ. Эле-менты эффективной и гибкой системы управления региональной системы ЗИ и основные вопросы, решаемые при её создании. Два вида про-блем. 1.3. Основные составляющие ИБ. Категории спектра интересов, свя-занных с использованием инф. си-стем. Понятия доступности, целост-ности и конфиденциальности, их смысл в контексте проблемы ИБ.

Тема 2. Концептуальные положения организационного обеспечения ИБ

устный опрос , примерные вопросы:

Реферат на тему "Организационное и правовое обеспечение информационной безопасности" 2.1. Общие сведения о доктрине и концепции организационного обеспе-чения безопасности. Цель и область применения концепции. Основания и исходные данные для разработки кон-цепции. 2.2. Задачи обеспечения нацио-нальной безопасности в информа-ционной сфере. Наиболее значимые задачи в гуманитарной области и в области обеспечения безопасности информационной инфраструктуры и ресурсов.

Тема 3. Информационная безопасность на объекте

устный опрос , примерные вопросы:

3.1 Угрозы ИБ на объекте. Источ-ники угроз безопасности. Деление источников угроз на группы, субъек-ты угроз. Виды угроз безопасности, классификация. Дополнительное де-ление на внутренние и внешние угро-зы. Каналы утечки информации. 3.2 Модель угроз безопасности на объекте. Методы защиты. Основ-ные группы методов (способов) за-щиты информации. Основные уровни защиты. 3.3 Принципы комплексной защи-ты информации. Основные принци-пы. Расшифровка понятий. 3.4 Система обеспечения ИБ, общие сведения об ИТКС. Стадии создания системы обеспечения безопасности. Организационные и технические мероприятия на каждой из стадий. Мероприятия, проводимые в процессе эксплуатации ИТКС. Понятие необходимого уровня защиты.

Тема 4. Конфиденциальная информация

устный опрос , примерные вопросы:

4.1. Организация службы безопас-ности объекта. Отношения объекта и субъекта в информационном про-цессе с противоположными интере-сами с позиции активности в дей-ствиях. Определение понятия утеч-ки информации. Уязвимые места в ИБ. Признаки наличия уязвимых мест. Примеры, способствующие неправомерному овладению конфи-денциальной информацией. Каналы, способы и средства. Формы и мето-ды недобросовестной конкуренции в контексте проблемы защиты ин-формации. Совокупность определе-ний, способов и средств НСД к ин-формации на объекте. 4.2. Направления обеспечения ИБ на объекте. Номативно-правовые категории. Направления обеспечения безопасности и защиты информации. Защитные действия и их характери-стики. Средства и методы организа-ционной защиты. Определение орга-низационной защиты. Состав меро-приятий организационной защиты. 4.3. Специальные штатные служ-бы и структуры ЗИ. Служба без-опасности предприятия, её струк-турные единицы. Задачи службы безопасности предприятия. 4.4. Концепция создания физиче-ской защиты важных объектов. Основные термины и определения. Система физической защиты, опре-деление. Деление СФЗ на подсисте-мы. Стадии проектирования объек-тов защиты. Основные этапы стадии концептуального проекта. Концеп-ция физической безопасности объ-екта. Основные вопросы концепции: предметы защиты, угрозы безопас-ности и модель вероятных исполни-телей угроз, оценка и анализ уязви-мости и общие рекомендации по обеспечению безопасности объекта. Меры физической безопасности.

Тема 5. Организационная структура и основные мероприятия по созданию и обеспечению функционирования комплексной системы ЗИ

устный опрос , примерные вопросы:

5.1. Цели, задачи и субъекты ИБ. Основные цели и задачи обеспечения ИБ. Управление ИБ. Классификация субъектов, влияющих на состояние ИБ. 5.2. Организационная структура системы обеспечения ИБ. Регла-ментация действий пользователей и обслуживающего персонала АС. Служба (подразделение) ЗИ. Уровни организационной структуры системы обеспечения ИБ АС организации. Технология обеспечения ИБ.

Тема 6. Система организационно-распорядительных документов по организации комплексной системы ЗИ

устный опрос , примерные вопросы:

6.1. Концепция обеспечения ИБ на предприятии. Документ Концепция обеспечения ИБ организации. Категорирование и перечень информационных ресурсов, подлежащих защите. Положение об определении требований по защите (категорировании) ресурсов. Классификация защищаемой информации. Инструкции по организации защиты.

Тема 7. Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО

устный опрос , примерные вопросы:

7.1. Задачи концептуального проектирования. Концептуальный проект. Оценка эффективности вариантов. 7.2. Создание службы безопасности организации. Разрешенные виды деятельности СБ. Организация службы экономической безопасности. Этапы, рекомендуемые при создании СЭБ.

Тема 8. Технология защиты от угроз экономической безопасности

устный опрос , примерные вопросы:

8.1. Общий алгоритм действий и активная модель реагирования. Последовательность операций (действий). Система предупредительных мер. Нестандартные угрозы. Активная модель реагирования. 8.2. Предупредительная работа с персоналом. Индикаторы выявления. Потенциальные нарушители. Проверки персонала, некоторые способы.

Тема 9. Требования и рекомендации по защите информации

устный опрос , примерные вопросы:

10.1. Требования по технической защите информации. Организация охраны объектов. 11.1. Организационно-пропускной режим на предприятии. 11.2. Подготовка исходных данных. 11.3. Оборудование пропускных пунктов. 11.4. Организация пропускного ре-жима. Система защиты информации и ее задачи. 12.1. Организационная система за-щиты информации. Государственная политика и об-щее руководство деятельностью по защите информации.

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

1. Правовые основы охраны коммерческой тайны.
2. Программные закладки и технологическая безопасность программного обеспечения (при разработке).
3. Технология разработки программного обеспечения.
4. Алгоритмические и программные закладки.
5. Объекты информационной системы, нуждающиеся в защите. Методика их выявления. Анализ рисков.
6. Классификация вирусов по режиму функционирования и объекту внедрения.
7. Аудит информационной безопасности.
8. Маршрутизация передачи сообщений в сети.
9. Трехуровневая структура организации обеспечения безопасности.
10. Криптографические алгоритмы защиты информации
11. Протоколы локальных сетей. Их назначение и виды.
12. Многоуровневая архитектура открытых систем.
13. Технология передачи пакетов в сетях.
14. Идентификация адреса абонента в сети и установление соединения.
15. Аппаратные средства защиты информации.
16. "Оранжевая книга": основные положения.
17. Обязательная конфиденциальная информация.
18. Типы компьютерных вирусов: классификация, свойства
19. Коммерчески значимая информация.
20. Аппаратные средства защиты информации.
21. Организация защиты информации в исследовательских учреждениях.
22. Распределение обязанностей и организация работы в подразделении, обеспечивающем защиту информации.
23. Операционные системы: назначение, основные функции,
24. Порядок и особенности внедрения КСИБ.
25. Порядок и особенности проведения испытаний и внедрения КСИБ.
26. Организация хранения документов.
27. Организационные проблемы защиты информации.
28. Аппаратные закладки, разновидности, способы обнаружения.
29. Правовая регламентация сертификационной деятельности в области защиты информации.
30. Компоненты комплексной системы защиты информации.
31. Поисковые работы при выявлении радиозакладных устройств.
32. Методика определения состава защищаемой информации. Перечень сведений, составляющих коммерческую тайну.
33. Механизмы обеспечения безопасности информации: идентификация, авторизация, аудит, разграничение доступа.
34. Информационное законодательство зарубежных стран.
35. Принципы построения комплексной системы защиты информации.
36. Разработка политики безопасности и регламенты информационной безопасности предприятия.
37. Управление проектами.
38. Правовые аспекты защиты информации.

39. Жизненный цикл информационной системы.

7.1. Основная литература:

Комплексная защита информации на предприятии. Т. 1, , 2012г.

Комплексная защита информации на предприятии. Т. 2, , 2012г.

Основы информационной безопасности, Расторгуев, Сергей Павлович, 2007г.

Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; 70x100 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4

- http://znanium.com/catalog.php?bookinfo=402686

Партыка Т. Л. Информационная безопасность: Учебное пособие для студентов учреждений среднего проф. обр. / Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - М.: Форум, 2008. - 432 с.: ил.; 60x90 1/16. - (Проф. обр.). (п) ISBN 978-5-91134-246
-http://znanium.com/catalog.php?bookinfo=167284

7.2. Дополнительная литература:

Комплексная защита информации на предприятии, Петровский, Владимир Ильич;Петровский, Владимир Владимирович;Глова, Виктор Иванович, 2012г.

Информационная безопасность и защита информации, Мельников, Владимир Павлович;Клейменов, С.А.;Петраков, А.М.;Клейменов, С.А., 2006г.

Правовая защита информации, Абзалов, Айрат Ринатович;Глова, Виктор Иванович;Зиновьев, Игорь Павлович, 2011г.

Информатика, автоматизированные информационные технологии и системы: Учебник / В.А. Гвоздева. - М.: ИД ФОРУМ: ИНФРА-М, 2011. - 544 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0449-7, 1500 экз. - http://znanium.com/bookread.php?book=207105

Аверченков, В. И. Аудит информационной безопасности [электронный ресурс] : учеб. пособие для вузов / В. И. Аверченков. - 2-е изд., стереотип. - М. : Флинта, 2011. - 269 с. - ISBN 978-5-9765-1256-6 - http://znanium.com/catalog.php?bookinfo=453734

7.3. Интернет-ресурсы:

Гарант - http://www.garant.ru/

Консультант Плюс - http://www.consultant.ru/

Официальный портал правовой информации - http://pravo.gov.ru/

Российская газета - http://www.rg.ru/

Собрание законодательства РФ - http://www.szrf.ru/

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Комплексное обеспечение информационной безопасности" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен студентам. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

стандартная аудитория с доской и мелом

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 090900.62 "Информационная безопасность" и профилю подготовки Информационная безопасность автоматизированных систем .

Автор(ы):
Ситников С.Ю. _____
"__" _____ 201 __ г.

Рецензент(ы):
Шерстюков О.Н. _____
"__" _____ 201 __ г.