МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Д.А. Таюрский
ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ (ДО КФУ)
«___»_____20__г.

подписано электронно-цифровой подписью

Программа дисциплины

Организационное и правовое обеспечение информационной безопасности Б1.Б.11

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Белашов В.Ю. , Ситников С.Ю.

Рецензент(ы):

Ситников Ю.К.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Шерстюков О. Н.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 935219

Содержание

Программу дисциплины разработал(а)(и) главный научный сотрудник, д.н. (профессор) Белашов В.Ю. НИЛ исследований ближнего космоса Институт физики , Vasilij.Belashov@kpfu.ru ; Ситников С.Ю. , ssitnikov@mail.ru

1. Цели освоения дисциплины

Целью освоения дисциплины (модуля) Организационное и правовое обеспечение информационной безопасности является получений знаний об организационно-правовых нормах и методах обеспечения информационной безопасности и защиты информации.

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

Данная учебная дисциплина включена в раздел "Б1.Б.11 Дисциплины (модули)" основной образовательной программы 10.03.01 Информационная безопасность и относится к базовой (общепрофессиональной) части. Осваивается на 2 курсе, 4 семестр.

Данная учебная дисциплина входит в раздел ФГОС ВО по направлению подготовки 'Информационная безопасность'.

Ее освоение предполагает наличие знаний и умений, сформированных в процессе изучения дисциплин: 'Основы теории права', 'Социология', 'Управление информационной безопасностью', 'Основы информационной безопасности'.

Полученные по данной дисциплине знания, умения и навыки используются в освоении дисциплин: 'Физические основы защиты информации', 'Программно-аппаратные средства защиты информации', 'Инженерно-техническая защита информации', 'Угрозы безопасности информационных систем', а также для последующего изучения других дисциплин вариативной части профессионального цикла.

Курс предназначен для студентов 2 года обучения, 2 семестр

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-3 (общекультурные компетенции)	способностью использовать основы правовых знаний в различных сферах жизнедеятельности
ОК-4 (общекультурные компетенции)	способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
ОПК-5 (профессиональные компетенции)	способностью использовать нормативные правовые акты в профессиональной деятельности
ПК-10 (профессиональные компетенции)	способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-16 (профессиональные компетенции)	способностью организовывать и поддерживать выполнение комплекса мер по обеспечению 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-17 (профессиональные компетенции)	способностью изучать и обобщать опыт работы различных учреждений, организаций и предприятий в области повышения эффективности защиты информации
ПК-20 (профессиональные компетенции)	способностью организовать технологический процесс защиты информации в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ПК-6 (профессиональные компетенции)	способностью принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия требованиям защиты информации

В результате освоения дисциплины студент:

1. должен знать:

должен знать основы:

- информационного законодательства РФ;
- системы защиты государственной тайны;
- правил лицензирования и сертификации в области защиты информации;
- международного законодательства в области защиты информации;
- знаний о компьютерных преступлениях;
- конституционные гарантии прав граждан на получение информации;
- организационного обеспечения безопасности информации,

2. должен уметь:

должен уметь:

- грамотно применять современную нормативно-правовую базу в области информационной безопасности;
- предлагать обоснованные варианты организационного обеспечения безопасности информации на конкретных объектах информационной защиты.
- пользоваться технологиями цифровой электронной подписи.

3. должен владеть:

владеть навыками в использовании существующих законов, норм и правил для решения практических задач обеспечения информационной безопасности.

4. должен демонстрировать способность и готовность:

осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности; разрабатывать предложения по совершенствованию системы управления информационной безопасностью; участвовать в работах по реализации политики информационной безопасности; применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) 108 часа(ов).

Форма промежуточного контроля дисциплины: зачет в 4 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	Практи-ческие занятия	Лабора-торные работы	
1.	Тема 1. Задачи и методы обеспечения ИБ. Проблема ИБ и основные составляющие ИБ. Информация конфиденциального характера. Стратегия ИБ и её цели. Административный уровень ИБ.	4	1-2	4	2	0	Письменная работа
2.	Тема 2. Концепция национальной безопасности РФ. Концептуальные положения организационного обеспечения ИБ. Задачи обеспечения национальной безопасности в информационной сфере. Методы работы с персоналом.	4	3	2	0	0	Письменная работа
3.	Тема 3. Угрозы ИБ на объекте. Модель угроз безопасности на объекте. Методы защиты. Принципы комплексной защиты информации. Система обеспечения ИБ в ИТКС.	4	4	2	2	0	Письменная работа
4.	Тема 4. Предпосылки появления угроз в ИТКС. Классификации угроз безопасности в ИТКС. Уязвимости.	4	5	2	0	0	Письменная работа

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практи-ческие занятия	Лабора-торные работы	
5.	Тема 5. Информационная безопасность на объекте. Концептуальная модель ИБ на объекте. Имитационное моделирование. Организационно-распорядительные документы по обеспечению ИБ. Концепция и политики ИБ на предприятии.	4	6	2	2	0	Устный опрос
6.	Тема 6. Организация службы безопасности объекта. Направления обеспечения ИБ на объекте. Специальные штатные службы и структуры ЗИ. Концепция создания физической защиты важных объектов.	4	7	2	0	0	Письменная работа
7.	Тема 7. Цели, задачи и субъекты ИБ. Организационная структура системы обеспечения ИБ. Основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты информации.	4	8	2	2	0	Коллоквиум
8.	Тема 8. Система организационно-распорядительных документов по организации комплексной системы ЗИ. Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО. Технология защиты от угроз экономической безопасности.	4	9-10	4	2	0	Письменная работа
9.	Тема 9. Подбор сотрудников и работа с кадрами.	4	11-12	4	2	0	Устный опрос
10.	Тема 10. Требования по технической защите информации. Организация охраны объектов.	4	13-14	4	2	0	Письменная работа
11.	Тема 11. Организационно-правовые вопросы нарушения ИБ.	4	15-16	4	2	0	Устный опрос
12.	Тема 12. Государственная политика и общее руководство деятельностью по защите информации.	4	17	2	0	0	Письменная работа

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
13.	Тема 13. Заключительное занятие. Основные документы нормативно-правовой базы организационного обеспечения информационной безопасности.	4	18	2	2	0	Коллоквиум
.	Тема . Итоговая форма контроля	4		0	0	0	Зачет
	Итого			36	18	0	

4.2 Содержание дисциплины

Тема 1. Задачи и методы обеспечения ИБ. Проблема ИБ и основные составляющие ИБ. Информация конфиденциального характера. Стратегия ИБ и её цели. Административный уровень ИБ.

лекционное занятие (4 часа(ов)):

Содержание основных используемых в ИБ понятий. Определение защиты информации. Основные методы обеспечения ИБ. Определение ИБ. Актуальные проблемы создания и совершенствования системы ЗИ. Элементы эффективной и гибкой системы управления региональной системы ЗИ и основные вопросы, решаемые при её создании. Два вида проблем. Категории спектра интересов, связанных с использованием инф. систем. Понятия доступности, целостности и конфиденциальности, их смысл в контексте проблемы ИБ. Перечень сведений конфиденциального характера. Определение стратегии ИБ и ее цели. Программа безопасности и политика безопасности. Процедурный уровень защиты. Уровни детализации политики безопасности, основные документы и их разделы.

практическое занятие (2 часа(ов)):

1. Концепция национальной безопасности РФ. 2. Об основах государственной политики в сфере информатизации (Указ № 170 от 20.01.94) 3. Закон РФ от 21 июля 1993 года № 5485-1 ?О Государственной тайне?. О перечне сведений, отнесенных к государственной тайне (новая редакция) (Указ № 90 от 11.02.2006) 4. Об утверждении перечня сведений конфиденциального характера (Указ № 188 от 06.03.97)

Тема 2. Концепция национальной безопасности РФ. Концептуальные положения организационного обеспечения ИБ. Задачи обеспечения национальной безопасности в информационной сфере. Методы работы с персоналом.

лекционное занятие (2 часа(ов)):

Доктрина и концепция безопасности. Нормативно-правовые документы. Цель и область применения концепции. Правовая основа и исходные данные для разработки концепции. Наиболее значимые задачи в гуманитарной области и в области обеспечения безопасности информационной инфраструктуры и ресурсов. 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. Угрозы ИБ на объекте. Модель угроз безопасности на объекте. Методы защиты. Принципы комплексной защиты информации. Система обеспечения ИБ в ИТКС.

лекционное занятие (2 часа(ов)):

Источники угроз безопасности. Деление источников угроз на группы, субъекты угроз. Виды угроз безопасности, классификация. Дополнительное деление на внутренние и внешние угрозы. Каналы утечки информации. Основные группы методов (способов) защиты информации. Основные уровни защиты. Основные принципы комплексной защиты информации. Расшифровка понятий. Стадии создания системы обеспечения безопасности ИТКС. Организационные и технические мероприятия на каждой из стадий. Мероприятия, проводимые в процессе эксплуатации ИТКС. Понятие необходимого уровня защиты.

практическое занятие (2 часа(ов)):

1. Федеральный закон Российской Федерации от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации". 2. Федеральный закон Российской Федерации от 29 июля 2004 года N 98-ФЗ ?О коммерческой тайне?. 3. Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных". 4. ИТКС и защита информации.

Тема 4. Предпосылки появления угроз в ИТКС. Классификации угроз безопасности в ИТКС. Уязвимости.

лекционное занятие (2 часа(ов)):

Предпосылки появления угроз в ИТКС, их возможные разновидности, интерпретация. Определение угрозы ИБ в ИТКС. Существующие классификации угроз и их источников в ИТКС. Классификация угроз безопасности в ИТКС по 5 группам различных угроз. Классифика-ция угроз в ИТКС по источнику возможной опасности. Классификация по защите информа-ции 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. Причины появления уязвимостей. Воздействия нарушителя на систему через её уязвимости на различных этапах функционирования ИТКС. Реализация угроз через КНПИ. Классификация КНПИ по двум критериям.

Тема 5. Информационная безопасность на объекте. Концептуальная модель ИБ на объекте. Имитационное моделирование. Организационно-распорядительные документы по обеспечению ИБ. Концепция и политики ИБ на предприятии.

лекционное занятие (2 часа(ов)):

Организационная защита в системе комплексной ЗИ. Основные цели и основные направления. Основные орг. мероприятия по созданию и обеспечению функционирования комплексной системы ЗИ. Определение ИБ. Четыре основные составляющие национальных интересов РФ в информационной сфере. Соблюдение конституционных прав и свобод человека и гражданина в области получения инф-ции и пользования ею. Информационное обеспечение государственной политики РФ. Развитие современных инф. технологий, отеч. индустрии информации, в т.ч. средств информатизации, телекоммуникации и связи. Защита инф. ресурсов от несанкц. доступа, обеспечение безопасности инф. и телекоммуникационных систем. Имитационное моделирование. Компоненты модели ИБ на 1 уровне. Основные компоненты системы управления ИБ организации. Пакет нормативных и организационно-распорядительных документов различного уровня. Концепция и политики ИБ на предприятии. Основные разделы концепции. Документы комплекта политик ИБ на предприятии в СУИБ. План развития системы ИБ на предпри-ятии, его основные разделы. Концептуальная модель безопасности информации организации (предприятия).

практическое занятие (2 часа(ов)):

1. Закон РФ "О правовой охране программ для электронных вычислительных машин и баз данных" (Закон РФ N 3523-1. Дата введения 23.09.92). 2. О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации (Указ № 334 от 03.04.95) 3. Нормативная регламентация использования криптографических средств кодирования информации. 4. Информационная безопасность на объекте. Имитационное моделирование.

Тема 6. Организация службы безопасности объекта. Направления обеспечения ИБ на объекте. Специальные штатные службы и структуры ЗИ. Концепция создания физической защиты важных объектов.

лекционное занятие (2 часа(ов)):

Отношения объекта и субъекта в информационном процессе с противоположными интересами с позиции активности в действиях. Определение понятия утечки информации. Уязвимые места в ИБ. Признаки наличия уязвимых мест. Примеры, способствующие неправомерному овладению конфиденциальной информацией. Каналы, способы и средства. Компьютерные преступления. Формы и методы недобросовестной конкуренции в контексте проблемы защиты информации. Совокупность определений, способов и средств НСД к информации на объекте. Направления обеспечения ИБ на объекте. Номативно-правовые категории. Направления обеспечения безопасности и защиты информации. Защитные действия и их характеристики. Средства и методы организационной защиты. Определение организационной защиты. Со-став мероприятий организационной защиты. Служба безопасности предприятия, её структурные единицы. Задачи службы безопасности предприятия. 28. Концепция создания физической защиты важных объектов. Основные термины и определения. Система физической защиты, определение. Деление СФЗ на подсистемы. Стадии проектирования объектов защиты. Основные этапы стадии концептуального проекта. Концепция физической безопасности объекта. Основные вопросы концепции: предметы защиты, угрозы безопасности и модель вероятных исполнителей угроз, оценка и анализ уязвимости и общие рекомендации по обеспечению безопасности объекта. Меры физической безопасности.

Тема 7. Цели, задачи и субъекты ИБ. Организационная структура системы обеспечения ИБ. Основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты информации.

лекционное занятие (2 часа(ов)):

Конечная цель ИБ и основная задача. Совокупность субъектов, влияющих на состояние ИБ. Регламентация действий пользователей и обслуживающего персонала АС. Совокупность уровней системы обеспечения ИБ АС. Понятие технологии обеспечения ИБ и её реализация. Организационные меры (мероприятия) по созданию и обеспечению функционирования комплексной системы защиты информации, их состав. Распределение функций по ИБ между подразделениями и отдельными сотрудниками. Служба безопасности, Управление автоматизации, ФАП.

практическое занятие (2 часа(ов)):

1. Указ Президента РФ от 17 марта 2008 г. № 351 ?О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена? (в ред. Указов Президента РФ от 21.10.2008 г. № 1510, от 14.01.2011 г. № 38). 2. Компьютерный терроризм.

Тема 8. Система организационно-распорядительных документов по организации комплексной системы ЗИ. Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО. Технология защиты от угроз экономической безопасности.

лекционное занятие (4 часа(ов)):

Концепция обеспечения ИБ на предприятии. Категорирование и перечень ин-формационных ресурсов, подлежащих защите. Перечень инструкций по организации защиты. Основные задачи концептуального проектирования. Правовые основы создания службы безопасности. Организация службы экономической безопасности, рекомендуемые этапы по её созданию. Структура СЭБ. Общий алгоритм действий и активная модель реагирования, отдельные её блоки, повышающие эффективность работы СЭБ. Предупредительная работа с персоналом, способы проверки персонала. Служба безопасности и проверка контрагентов. Криминалистическая экспертиза документов.

практическое занятие (2 часа(ов)):

1. Правовая регламентация сертификационной деятельности в области защиты информации.
2. Органы сертификации в информационной сфере и их полномочия.

Тема 9. Подбор сотрудников и работа с кадрами.

лекционное занятие (4 часа(ов)):

Подбор сотрудников и работа с кадрами. Концептуальные подходы к обеспечению безопасности. Методы сбора информации при планировании противоправных действий. Обеспечение безопасности коммерческих структур. Особенности психологических подходов к профотбору. Этапы психологического профотбора. Тестовые процедуры проверки кандидатов. Личностные опросные листы. Бланковые, проективные и приборные методики. Процедуры отбора кандидатов по итогам тестирований. Заключительное собеседование. Особенности проверки руководящих кадров. Процесс увольнения кадров. Основные принци-пы в работе с кадрами. Организация внутриобъектового режима. Основные задачи группы режима.

практическое занятие (2 часа(ов)):

1. Трудовое законодательство в части приема на работу и увольнения. 2. Приказ ФСТЭК РФ № 58 ? об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных.

Тема 10. Требования по технической защите информации. Организация охраны объектов.

лекционное занятие (4 часа(ов)):

Защита информации при реализации информационных процессов. Эксплуатация компьютерного оборудования. Проблемы с электропитанием. Нестабильная работа ОС. Неквалифицированные действия пользователей. Резервное копирование. Контрольно-пропускной режим на предприятии. Основные цели создания КПР и задачи КПР. Нормативные, организационные и материальные гарантии. Подготовка исходных данных. Последовательность определения и оценки исходных данных. Инструкция о пропускном режиме, её разделы. Виды пропусков. Оборудование пропускных пунктов. Транспортные КПП. Организация пропускного режима. Пропускные документы. СО и КД, структурная схема. Идентификаторы, их классификация.

практическое занятие (2 часа(ов)):

1. Нормативная база по обеспечению КПР на предприятии. 2. Приказ Министерства Российской Федерации по связи и информатизации от 25 июля 2000 г. № 130 ?О порядке внедрения системы технических средств по обеспечению оперативно-розыскных мероприятий на сетях телефонной, подвижной и беспроводной связи и персонального радиовызова общего пользования?. 3. Постановление Правительства РФ от 27 августа 2005 г. № 538 ?Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность? и ?Правила?. 4. Защита информации в корпоративных информационных системах. 5. Классификация компьютерных вирусов: зоны поражения и меры защиты.

Тема 11. Организационно-правовые вопросы нарушения ИБ.

лекционное занятие (4 часа(ов)):

Нарушения безопасности информации. Результаты реализации угроз ИБ. Основные объекты защиты. Задачи по защите информации, определяемые концепцией ЗИ. Цель и задачи защиты информации, сферы, в которых они решаются. Основные направления деятельности по защите информации. Основы организации защиты информации. Особенности организации ЗИ, соответствующие цели и направления защиты. Организация контроля состояния системы ЗИ. Система защиты информации и её задачи. Уровни организационной системы защиты информации.

практическое занятие (2 часа(ов)):

1. IT-безопасность. Киберполиция - Управление ?К? БСТМ МВД России. 2. Статья 272 УК РФ ?Неправомерный доступ к компьютерной информации? и комментарии к статье. 3. Компьютерные правонарушения (ст. 274 УК РФ с комментариями). 4. Свободно распространяемое программное обеспечение и его защищенность. 5. Безопасность электронной почты.

Тема 12. Государственная политика и общее руководство деятельностью по защите информации.

лекционное занятие (2 часа(ов)):

Органы и лица, осуществляющие гос. политику и общее руководство деятельностью по ЗИ. Направления формирования системы ЗИ, основные принципы формирования и развития. Этапы реализации концепции ЗИ в федеральном округе, основные задачи этапов. Фи-нансирование мероприятий по ЗИ. Результаты реализации концепции ЗИ.

Тема 13. Заключительное занятие. Основные документы нормативно-правовой базы организационного обеспечения информационной безопасности.

лекционное занятие (2 часа(ов)):

Обобщение пройденного материала. Конкретизация документов нормативно-правовой базы по информационной безопасности и защите информации. Перечень основных нормативно-правовых документов.

практическое занятие (2 часа(ов)):

1. О мерах по совершенствованию государственного управления в области безопасности Российской Федерации (Указ 11 марта 2003 года № 308) (Упраздняет Гостехкомиссию и ФАПСИ). 2. Стратегия национальной безопасности РФ до 2020 года (утв. Указом Президента РФ от 12.05.2009 г. № 537).

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел дисциплины	Се-местр	Неде-ля семе стра	Виды самостоятельной работы студентов	Трудо-емкость (в часах)	Формы контроля самосто-ятельной работы
1.	Тема 1. Задачи и методы обеспечения ИБ. Проблема ИБ и основные составляющие ИБ. Информация конфиденциального характера. Стратегия ИБ и её цели. Административный уровень ИБ.	4	1-2	подготовка к письменной работе	2	Пись-мен-ная работа
2.	Тема 2. Концепция национальной безопасности РФ. Концептуальные положения организационного обеспечения ИБ. Задачи обеспечения национальной безопасности в информационной сфере. Методы работы с персоналом.	4	3	подготовка к письменной работе	4	Пись-мен-ная работа

N	Раздел дисциплины	Се-местр	Неде-ля семе стра	Виды самостоятельной работы студентов	Трудо-емкость (в часах)	Формы контроля самосто-ятельной работы
3.	Тема 3. Угрозы ИБ на объекте. Модель угроз безопасности на объекте. Методы защиты. Принципы комплексной защиты информации. Система обеспечения ИБ в ИТКС.	4	4	подготовка к письменной работе	4	Пись-мен-ная работа
4.	Тема 4. Предпосылки появления угроз в ИТКС. Классификации угроз безопасности в ИТКС. Уязвимости.	4	5	подготовка к письменной работе	2	Пись-мен-ная работа
5.	Тема 5. Информационная безопасность на объекте. Концептуальная модель ИБ на объекте. Имитационное моделирование. Организационно-распорядительные документы по обеспечению ИБ. Концепция и политики ИБ на предприятии.	4	6	подготовка к устному опросу	4	Устный опрос

N	Раздел дисциплины	Се-местр	Неде-ля семе стра	Виды самостоятельной работы студентов	Трудо-емкость (в часах)	Формы контроля самосто-ятельной работы
6.	Тема 6. Организация службы безопасности объекта. Направления обеспечения ИБ на объекте. Специальные штатные службы и структуры ЗИ. Концепция создания физической защиты важных объектов.	4	7	подготовка к письменной работе	2	Пись-мен-ная работа
7.	Тема 7. Цели, задачи и субъекты ИБ. Организационная структура системы обеспечения ИБ. Основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты информации.	4	8	подготовка к коллоквиуму	8	Коллоквиум
8.	Тема 8. Система организационно-распорядительных документов по организации комплексной системы ЗИ. Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО. Технология защиты от угроз экономической безопасности.	4	9-10	подготовка к письменной работе	4	Пись-мен-ная работа
9.	Тема 9. Подбор сотрудников и работа с кадрами.	4	11-12	подготовка к устному опросу	4	Устный опрос

N	Раздел дисциплины	Се-местр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
10.	Тема 10. Требования по технической защите информации. Организация охраны объектов.	4	13-14	подготовка к письменной работе	4	Письменная работа
11.	Тема 11. Организационно-правовые вопросы нарушения ИБ.	4	15-16	подготовка к устному опросу	4	Устный опрос
12.	Тема 12. Государственная политика и общее руководство деятельностью по защите информации.	4	17	подготовка к письменной работе	4	Письменная работа
13.	Тема 13. Заключительное занятие. Основные документы нормативно-правовой базы организационного обеспечения информационной безопасности.	4	18	подготовка к коллоквиуму	8	Коллоквиум
	Итого				54	

5. Образовательные технологии, включая интерактивные формы обучения

Используются такие интерактивные формы обучения, как чтение лекций с использованием мультимедиа оборудования, подготовка студентами компьютерных презентаций и выступление с ними на практических (семинарских) занятиях.

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

Тема 1. Задачи и методы обеспечения ИБ. Проблема ИБ и основные составляющие ИБ. Информация конфиденциального характера. Стратегия ИБ и её цели. Административный уровень ИБ.

Письменная работа , примерные вопросы:

Основными задачами системы ИБ являются: -своевременное выявление и устранение угроз безопасности и ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба его интересам; -создание механизма и условий оперативного реагирования на угрозы безопасности и проявлению негативных тенденций в функционировании предприятия; -эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности; -создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на достижение целей организации.

Тема 2. Концепция национальной безопасности РФ. Концептуальные положения организационного обеспечения ИБ. Задачи обеспечения национальной безопасности в информационной сфере. Методы работы с персоналом.

Письменная работа , примерные вопросы:

В Концепции национальной безопасности РФ, утвержденной Указом Президента РФ от 17.12.1997 г. № 1300 (в редакции Указа Президента РФ от 10.01.2000 г. №24), дается следующее определение национальной безопасности. Под национальной безопасностью РФ понимается безопасность ее многонационального народа как носителя суверенитета и единственного источника власти в РФ. Национальные интересы России - это совокупность сбалансированных интересов личности, общества и государства в различных сферах жизнедеятельности: экономической, внутриполитической, социальной, международной, информационной, военной, пограничной, экологической и других. В теории национальной безопасности используется понятие "жизненно важные интересы". Жизненно важные интересы - это совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства. Национальные интересы носят долгосрочный характер. В области внутренней и внешней политики государства этими интересами определяются: - основные цели этой политики; - стратегические и текущие задачи. Национальные интересы обеспечиваются институтами государственной власти, осуществляющими свои функции, в том числе во взаимодействии с действующими на основе Конституции РФ и законодательства РФ общественными организациями.

Тема 3. Угрозы ИБ на объекте. Модель угроз безопасности на объекте. Методы защиты. Принципы комплексной защиты информации. Система обеспечения ИБ в ИТКС.

Письменная работа , примерные вопросы:

Для описания угроз безопасности, которым подвержена информационная система, используется Модель угроз безопасности информации. Модель угроз является одним из основополагающих документов при построении системы защиты конкретной информационной системы, так как именно в ней учитываются особенности ИС, используемые в ней программные, программно-технические средства и процессы обработки информации. В 2015 г. ФСТЭК России опубликовала проект документа - "Методика определения угроз безопасности информации в информационных системах" (далее Методика). В ближайшем будущем он должен заменить "Методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 14.02.2008. Процесс определения угроз безопасности информации Методики, в отличие от действующего руководящего документа, делится на четыре этапа: Область применения процесса определения угроз безопасности информации. Идентификация угроз безопасности информации и их источников. Определение актуальных угроз безопасности информации. Мониторинг и переоценка угроз безопасности информации. Определение угроз безопасности информации должно осуществляться не только на этапе создания информационной системы и формирования требований к ней, но и в ходе эксплуатации.

Тема 4. Предпосылки появления угроз в ИТКС. Классификации угроз безопасности в ИТКС. Уязвимости.

Письменная работа , примерные вопросы:

Источники угрозы информационной безопасности: несанкционированный доступ к информационным базам, программные и физические воздействия, вызывающие потери и /или/ разрушения информации (ее носителей). Спектр угроз информационной безопасности весьма широк. Потеря (разрушение) информации может произойти по разным причинам, в том числе: ? нарушение работы компьютера; отключение или сбои питания; авария, взрыв, пожар, наводнение, техногенная катастрофа, иные чрезвычайные обстоятельства, ситуации, террористические акты, стихийные бедствия; ? повреждение носителей информации; действие компьютерных вирусов, иных вредоносных программ; ошибочные действия пользователей; ? несанкционированные умышленные действия других лиц, использующих разнообразные приемы [например, аналитической, конкурентной, технической или иной разведки, промышленного шпионажа, включая ?классические? методы шпионажа - шантаж, подкуп, психологический террор и т.п.].

Тема 5. Информационная безопасность на объекте. Концептуальная модель ИБ на объекте. Имитационное моделирование. Организационно-распорядительные документы по обеспечению ИБ. Концепция и политики ИБ на предприятии.

Устный опрос , примерные вопросы:

Концептуальная модель безопасности информации может содержать следующие компоненты: -объекты угроз; -угрозы информации; -источники угроз; -цели угроз со стороны злоумышленников; -источники информации; -способы защиты информации; -средства защиты информации; -направления защиты информации; -способы доступа к информации (способы неправомерного овладения информацией). Объектом угроз информационной безопасности выступают сведения о составе, состоянии и деятельности объекта защиты (персонала, ма�териальных и финансовых ценностей, информационных ресурсов). Угрозы информации выражаются в нарушении ее целостности, конфиденциальности, достоверности и доступности. Источниками угроз выступают конкуренты, преступники, корруп�ционеры, административные органы. Целями угрозявляются ознаком�ление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба. Источниками информации являются люди, доку�менты, публикации, технические носители информации, техниче�ские средства обеспечения производственной и трудовой деятель�ности, продукция и отходы производства. Способы защиты включают всевозможные меры и действия, обеспечивающие упреждение противоправных действий, их предотвращение, пресечение и противодействие не�санкционированному доступу. Средствами защиты информации являются физические средства, аппаратные средства, программные средства, криптографические и стеганографические методы. Последние два метода могут быть реализованы аппаратными, программ�ными и аппаратно-программными средствами. Направлениями защиты информации являются правовая, организационная и инженерно-техническая защита как выразители комплексного подхода к обеспечению информационной безопасности. Способы доступа к информации возмож�ны за счет ее разглашения источниками сведений, за счет утечки информации через технические средства и за счет несанкциониро�ванного доступа к охраняемым сведениям.

Тема 6. Организация службы безопасности объекта. Направления обеспечения ИБ на объекте. Специальные штатные службы и структуры ЗИ. Концепция создания физической защиты важных объектов.

Письменная работа , примерные вопросы:

Основными задачами службы безопасности предприятия являются: обеспечение безопасности производственно-торговой деятельности и защиты информации и сведений, являющихся коммерческой тайной; организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны; организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной; предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим коммерческую тайну; выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях; обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, заседания, связанные с деловым сотрудничеством как на национальном, так и на международном уровне; обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности; обеспечение личной безопасности руководства и ведущих сотрудников и специалистов; оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.

Тема 7. Цели, задачи и субъекты ИБ. Организационная структура системы обеспечения ИБ. Основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты информации.

Коллоквиум , примерные вопросы:

Реализация технологии обеспечения безопасности ИТ предполагает: назначение и подготовку должностных лиц (сотрудников), ответственных за организацию, реализацию функций и осуществление конкретных практических мероприятий по обеспечению безопасности информации и процессов её обработки; строгий учёт всех подлежащих защите ресурсов системы (информации, её носителей, процессов обработки) и определение требований к организационно-техническим мерам и средствам их защиты; разработку реально выполнимых и непротиворечивых организационно-распорядительных документов по вопросам обеспечения безопасности информации; реализацию (реорганизацию) технологических процессов обработки информации в АС с учётом требований по безопасности ИТ; принятие эффективных мер сохранности и обеспечения физической целостности технических средств и поддержку необходимого уровня защищённости компонентов АС; применение физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывную административную поддержку их использования; регламентацию всех процессов обработки подлежащей защите информации, с применением средств автоматизации и действий сотрудников структурных подразделений, использующих АС, а также действий персонала, осуществляющего обслуживание и модификацию программных и технических средств АС, на основе утверждённых организационно- распорядительных документов по вопросам обеспечения безопасности ИТ; чёткое знание и строгое соблюдение всеми сотрудниками, использующими и обслуживающими аппаратные и программные средства АС, требований организационно-распорядительных документов по вопросам обеспечения безопасности информации; персональную ответственностью за свои действия каждого сотрудника, участвующего в рамках своих функциональных обязанностей, в процессах автоматизированной обработки информации и имеющего доступ к ресурсам АС; эффективный контроль за соблюдением сотрудниками подразделений - пользователями и обслуживающим АС персоналом, ? требований по обеспечению безопасности информации; проведение постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработку и реализацию предложений по совершенствованию системы защиты информации в АС.

Тема 8. Система организационно-распорядительных документов по организации комплексной системы ЗИ. Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО. Технология защиты от угроз экономической безопасности.

Письменная работа , примерные вопросы:

В соответствии с приказом ФСТЭК России от 11.02.2013 № 17 ?Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах? на этапе внедрения системы защиты информации в информационную систему разрабатываются организационно-распорядительные документы по защите информации. 1. Перечень информационных систем и информации ограниченного доступа 2. Перечень лиц, допущенных к обработке информации 3. Приказ о назначении ответственного за защиту информации 4. Правила обращения с машинными носителями информации 5. Инструкция по антивирусной защите 6. Инструкция по организации парольной защиты 7. Инструкция по резервному копированию 8. Инструкция администратора ИБ 9. Инструкция пользователя ИС

Тема 9. Подбор сотрудников и работа с кадрами.

Устный опрос , примерные вопросы:

Система подбора персонала предусматривает тщательное изучение потребностей работодателя и предложений рынка труда. Только тогда, когда будут выяснены все требования к кандидату, особенности вакантной должности и другие немаловажные нюансы, можно формировать список претендентов. Из всех возможных предложений сразу отсеиваются неподходящие по уровню квалификации работники, служащие, имеющие плохую репутацию и негативные отзывы с предыдущих мест работы, лица, совершавшие правонарушения, кандидаты, не удовлетворяющие всем требованиям работодателя, лица, квалификация которых не соответствует запрашиваемому уровню заработной платы. Таким образом, систем позволяет составить оптимизированный список кандидатов, которые способны занимать искомую вакансию. Эта стратегия значительно экономит время, личные встречи и собеседования проводятся только с соискателями, прошедшими первый этап отбора.

Тема 10. Требования по технической защите информации. Организация охраны объектов.

Письменная работа , примерные вопросы:

Основными организационно-техническими мероприятиями по защите информации являются: лицензирование деятельности предприятий в области защиты информации; разработка средств защиты информации и контроля за ее эффективностью и их использование; сертификация средств защиты информации и контроля за ее эффективностью; создание и применение автоматизированных информационных систем в защищенном исполнении; аттестация объектов и систем информатизации на соответствие требованиям безопасности информации при проведении работ со сведениями соответствующей степени секретности.

Тема 11. Организационно-правовые вопросы нарушения ИБ.

Устный опрос , примерные вопросы:

Организационно-правовое обеспечение информационной безопасности представляет собою совокупность решений, законов, нормативов, регламентирующих как общую организацию работ по обеспечению информационной безопасности, так и создание и функционирование систем защиты информации на конкретных объектах. Поэтому организационно-правовая база должна обеспечивать основные функции: 1) разработка основных принципов отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации; 2) определение системы органов и должностных лиц, ответственных за обеспечение информационной безопасности в стране и порядка регулирования деятельности предприятий и организаций в этой области; 3) создание полного комплекса нормативно-правовых руководящих и методических материалов (документов), регламентирующих вопросы обеспечения информационной безопасности как в стране в целом, так и на конкретном объекте; 4) определение мер ответственности за нарушение правил защиты; 5) определение порядка разрешения спорных и конфликтных ситуаций по вопросам защиты информации.

Тема 12. Государственная политика и общее руководство деятельностью по защите информации.

Письменная работа , примерные вопросы:

Государственная политика обеспечения информационной безопасности основывается на следующих принципах: ? соблюдения Конституции РФ, законодательство РФ, общепринятых законов и норм международного права; ? открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов РФ, с учётом ограничений, установленных законодательством РФ; ? правовое равенство всех участников процесса информационного взаимодействия, основывающего на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации; ? приоритетное развитие отечественных, современных, информационных и телекоммуникационных технологий, производство технических и программных средств для соблюдения жизненно важных интересов Российской Федерации.

Тема 13. Заключительное занятие. Основные документы нормативно-правовой базы организационного обеспечения информационной безопасности.

Коллоквиум , примерные вопросы:

Отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников отношений, в том числе государства, на рынке товаров, работ и услуг, регулируются ФЗ от 29.07.2004 № 98-ФЗ ?О коммерческой тайне?. К нормативным актам данной проблематики относятся федеральные законы: - от 13.01.1995 № 7-ФЗ ?О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации?; - от 12.05.2009 № 95-ФЗ ?О гарантиях равенства парламентских партий при освещении их деятельности государственными общедоступными телеканалами и радиоканалами?; - от 27.07.2006 № 152-ФЗ ?О персональных данных?; - от 28.12.2010 № 390-ФЗ ?О безопасности?; Среди подзаконных нормативных актов, регулирующих отношения в информационной сфере, можно выделить следующие: указы Президента: ? от 11.02.2006 № 90 ?О перечне сведений, отнесенных к государственной тайне?; ? от 06.10.2004 № 1286 ?Вопросы межведомственной комиссии по защите государственной тайны?; ? от 17.05.2004 № 611 ?О мерах по обеспечению безопасности РФ в сфере международного информационного обмена?; ? от 06.03.1997 № 188 ?Об утверждении Перечня сведений конфиденциального характера?; ? от 15.01.2913 № 31/с ?О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ?.

Итоговая форма контроля

зачет (в 4 семестре)

Примерные вопросы к зачету:

Для аттестации студентов проводятся устные опросы, коллоквиумы и зачет.

На практических занятиях рассматриваются вопросы теории и практики методов и форм организационного и правого обеспечения информационной безопасности, положения основных нормативно-правовых документов в виде индивидуальных докладов-презентаций студентов с дискуссией по разделам курса.

ВОПРОСЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Концепция национальной безопасности РФ.

2. Закон РФ от 21 июля 1993 года № 5485-1 "О Государственной тайне".

3. Федеральный закон Российской Федерации от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

4. Федеральный закон Российской Федерации от 29 июля 2004 года N 98-ФЗ "О коммерческой тайне".

5. Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных".

6. Закон РФ "О правовой охране программ для электронных вычислительных машин и баз данных" (Закон РФ N 3523-1. Дата введения 23.09.92).

7. Об основах государственной политики в сфере информатизации (Указ № 170 от 20.01.94)

8. О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации (Указ № 334 от 03.04.95)

9. О перечне сведений, отнесенных к государственной тайне (новая редакция) (Указ № 90 от 11.02.2006)

10. Об утверждении перечня сведений конфиденциального характера (Указ № 188 от 06.03.97)

11. О мерах по совершенствованию государственного управления в области безопасности Российской Федерации (Указ 11 марта 2003 года № 308) (Упраздняет Гостехкомиссию и ФАПСИ).

12. Трудовое законодательство в части приема на работу и увольнения.

13. Нормативная регламентация использования криптографических средств кодирования информации.

14. Нормативная база по обеспечению КПР на предприятии.

15. ИТКС и защита информации.

16. Стратегия национальной безопасности РФ до 2020 года (утв. Указом Президента РФ от 12.05.2009 г. № 537).

17. Информационная безопасность на объекте. Имитационное моделирование.

18. Приказ ФСТЭК РФ № 58 - об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных.

19. IT-безопасность. Киберполиция - Управление "К" БСТМ МВД России.

20. Статья 272 УК РФ "Неправомерный доступ к компьютерной информации" и комментарии к статье.

21. Постановление Правительства РФ от 27 августа 2005 г. № 538 "Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность" и "Правила".

22. Правовая регламентация сертификационной деятельности в области защиты информации.

23. Указ Президента РФ от 17 марта 2008 г. № 351 "О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена" (в ред. Указов Президента РФ от 21.10.2008 г. № 1510, от 14.01.2011 г. № 38).

24. Органы сертификации в информационной сфере и их полномочия.

25. Приказ Министерства Российской Федерации по связи и информатизации от 25 июля 2000 г. № 130 "О порядке внедрения системы технических средств по обеспечению оперативно-розыскных мероприятий на сетях телефонной, подвижной и беспроводной связи и персонального радиовызова общего пользования".

26. Компьютерные правонарушения (ст. 274 УК РФ с комментариями).

27. Пластиковые карты, как канал утечки информации.

28. Свободно распространяемое программное обеспечение и его защищенность.

29. Компьютерный терроризм. (Набережных)

30. Безопасность электронной почты.

31. Защита информации в корпоративных информационных системах. (Егоров)

32. Классификация компьютерных вирусов: зоны поражения и меры защиты. (Рыжова Ася)

33. Троянский вирус: принципы действия и этапы защиты.

ВОПРОСЫ К ЗАЧЕТУ

1. Задачи и методы обеспечения ИБ. Содержание основных используемых в ИБ понятий. Определение защиты информации. Основные методы обеспечения ИБ.

2. Проблема ИБ. Определение ИБ. Актуальные проблемы создания и совершенствования сис-темы ЗИ. Элементы эффективной и гибкой системы управления региональной системы ЗИ и основные вопросы, решаемые при её создании. Два вида проблем.

3. Основные составляющие ИБ. Категории спектра интересов, связанных с использованием инф. систем. Понятия доступности, целостности и конфиденциальности, их смысл в контек-сте проблемы ИБ.

4. Информация конфиденциального характера. Определение. Основные нормативно-правовые документы. Перечень сведений конфиденциального характера.

5. Стратегия ИБ и её цели. Определение понятия. Главные цели ИБ.

6. Административный уровень ИБ. Программа безопасности и политика безопасности. Про-цедурный уровень защиты. Уровни детализации политики безопасности, основные документы и их разделы.

7. Концепция национальной безопасности РФ и ФЗ РФ № 149-ФЗ "Об информации, ин-формационных технологиях и защите информации". Основные положения документов.

8. Концептуальные положения организационного обеспечения ИБ. Доктрина и концепция безопасности. Нормативно-правовые документы. Цель и область применения концепции. Правовая основа и исходные данные для разработки концепции.

9. Задачи обеспечения национальной безопасности в информационной сфере. Наиболее значимые задачи в гуманитарной области и в области обеспечения безопасности информационной инфраструктуры и ресурсов.

10. 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.

11. Закон РФ № 5485-1 "О Государственной тайне" и Указ № 170 "Об основах государственной политики в сфере информатизации".

12. Угрозы ИБ на объекте. Источники угроз безопасности. Деление источников угроз на группы, субъекты угроз. Виды угроз безопасности, классификация. Дополнительное деление на внутренние и внешние угрозы. Каналы утечки информации.

13. Модель угроз безопасности на объекте. Методы защиты. Основные группы методов (способов) защиты информации. Основные уровни защиты.

14. Принципы комплексной защиты информации. Основные принципы. Расшифровка понятий.

15. Система обеспечения ИБ в ИТКС. Стадии создания системы обеспечения безопасности ИТКС. Организационные и технические мероприятия на каждой из стадий. Мероприятия, проводимые в процессе эксплуатации ИТКС. Понятие необходимого уровня защиты.

16. Предпосылки появления угроз в ИТКС, их возможные разновидности, интерпретация. Определение угрозы ИБ в ИТКС. Существующие классификации угроз и их источников в ИТКС.

17. Классификация угроз безопасности в ИТКС по 5 группам различных угроз. Классифика-ция 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.

18. Уязвимости. Причины появления уязвимостей. Воздействия нарушителя на систему через её уязвимости на различных этапах функционирования ИТКС. Реализация угроз через КНПИ. Классификация КНПИ по двум критериям.

19. Информационная безопасность на объекте. Организационная защита в системе комплексной ЗИ. Основные цели и основные направления. Основные орг. мероприятия по созданию и обеспечению функционирования комплексной системы ЗИ.

20. Концептуальная модель ИБ на объекте. Определение ИБ. Четыре основные составляющие национальных интересов РФ в информационной сфере. Соблюдение конституционных прав и свобод человека и гражданина в области получения инф-ции и пользования ею. Информационное обеспечение государственной политики РФ. Развитие современных инф. технологий, отеч. индустрии информации, в т.ч. средств информатизации, телекоммуникации и связи. Защита инф. ресурсов от несанкц. доступа, обеспечение безопасности инф. и телекоммуникационных систем.

21. Имитационное моделирование. Компоненты модели ИБ на 1 уровне.

22. Организационно-распорядительные документы по обеспечению ИБ. Основные компоненты системы управления ИБ организации. Пакет нормативных и организационно-распорядительных документов различного уровня.

23. Концепция и политики ИБ на предприятии. Основные разделы концепции. Документы комплекта политик ИБ на предприятии в СУИБ. План развития системы ИБ на предприятии, его основные разделы. Концептуальная модель безопасности информации организации (предприятия).

24. Организация службы безопасности объекта. Отношения объекта и субъекта в информационном процессе с противоположными интересами с позиции активности в действиях. Определение понятия утечки информации.

25. Организация службы безопасности объекта. Уязвимые места в ИБ. Признаки наличия уязвимых мест. Примеры, способствующие неправомерному овладению конфиденциальной информацией. Каналы, способы и средства. Компьютерные преступления. Формы и методы недобросовестной конкуренции в контексте проблемы защиты информации. Совокупность определений, способов и средств НСД к информации на объекте.

26. Направления обеспечения ИБ на объекте. Номативно-правовые категории. Направления обеспечения безопасности и защиты информации. Защитные действия и их характеристики. Средства и методы организационной защиты. Определение организационной защиты. Со-став мероприятий организационной защиты.

27. Специальные штатные службы и структуры ЗИ. Служба безопасности предприятия, её структурные единицы. Задачи службы безопасности предприятия.

28. Концепция создания физической защиты важных объектов. Основные термины и определения. Система физической защиты, определение. Деление СФЗ на подсистемы. Стадии проектирования объектов защиты. Основные этапы стадии концептуального проекта. Концепция физической безопасности объекта. Основные вопросы концепции: предметы защиты, угрозы безопасности и модель вероятных исполнителей угроз, оценка и анализ уязвимости и общие рекомендации по обеспечению безопасности объекта. Меры физической безопасности.

29. Цели, задачи и субъекты ИБ. Конечная цель и основная задача. Совокупность субъектов, влияющих на состояние ИБ.

30. Организационная структура системы обеспечения ИБ. Регламентация действий пользователей и обслуживающего персонала АС. Совокупность уровней системы обеспечения ИБ АС. Понятие технологии обеспечения ИБ и её реализация.

31. Основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты информации. Организационные меры (мероприятия), их состав. Распределение функций по ИБ между подразделениями и отдельными сотрудниками. Служба безопасности, Управление автоматизации, ФАП.

32. Система организационно-распорядительных документов по организации комплексной системы ЗИ. Концепция обеспечения ИБ на предприятии. Категорирование и перечень информационных ресурсов, подлежащих защите. Перечень инструкций по организации защиты.

33. Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО. Основные задачи концептуального проектирования. Правовые основы создания службы безопасности. Организация службы экономической безопасности, рекомендуемые этапы по её созданию. Структура СЭБ.

34. Технология защиты от угроз экономической безопасности. Общий алгоритм действий и активная модель реагирования, отдельные её блоки, повышающие эффективность работы СЭБ. Предупредительная работа с персоналом, способы проверки персонала. Служба безопасности и проверка контрагентов. Криминалистическая экспертиза документов.

35. Подбор сотрудников и работа с кадрами. Концептуальные подходы к обеспечению безопасности. Методы сбора информации при планировании противоправных действий.

36. Подбор сотрудников и работа с кадрами. Обеспечение безопасности коммерческих структур. Особенности психологических подходов к профотбору. Этапы психологического профотбора.

37. Подбор сотрудников и работа с кадрами. Тестовые процедуры проверки кандидатов. Лич-ностные опросные листы. Бланковые, проективные и приборные методики. Процедуры от-бора кандидатов по итогам тестирований. Заключительное собеседование. Особенности проверки руководящих кадров.

38. Подбор сотрудников и работа с кадрами. Процесс увольнения кадров. Основные принципы в работе с кадрами.

39. Подбор сотрудников и работа с кадрами. Организация внутриобъектового режима. Ос-новные задачи группы режима.

40. Требования по технической защите информации. Защита информации при реализации информационных процессов. Эксплуатация компьютерного оборудования. Проблемы с электропитанием. Нестабильная работа ОС. Неквалифицированные действия пользователей. Резервное копирование.

41. Организация охраны объектов. Контрольно-пропускной режим на предприятии. Основные цели создания КПР и задачи КПР. Нормативные, организационные и материальные гарантии.

42. Организация охраны объектов. Подготовка исходных данных. Последовательность опре-деления и оценки исходных данных. Инструкция о пропускном режиме, её разделы. Виды пропусков.

43. Организация охраны объектов. Оборудование пропускных пунктов. Транспортные КПП.

44. Организация охраны объектов. Организация пропускного режима. Пропускные документы. СО и КД, структурная схема. Идентификаторы, их классификация.

45. Организационно-правовые вопросы нарушения ИБ. Нарушения безопасности информации. Результаты реализации угроз ИБ. Основные объекты защиты. Задачи по защите информации, определяемые концепцией ЗИ.

46. Организационно-правовые вопросы нарушения ИБ. Цель и задачи защиты информации, сферы, в которых они решаются. Основные направления деятельности по защите информации.

47. Организационно-правовые вопросы нарушения ИБ. Основы организации защиты ин-формации. Особенности организации ЗИ, соответствующие цели и направления защиты.

48. Организационно-правовые вопросы нарушения ИБ. Организация контроля состояния системы ЗИ. Система защиты информации и её задачи. Уровни организационной системы защиты информации.

49. Государственная политика и общее руководство деятельностью по защите информа-ции. Органы и лица, осуществляющие гос. политику и общее руководство деятельностью по ЗИ. Направления формирования системы ЗИ, основные принципы формирования и развития.

50. Государственная политика и общее руководство деятельностью по защите информа-ции. Этапы реализации концепции ЗИ в федеральном округе, основные задачи этапов. Финансирование мероприятий по ЗИ. Результаты реализации концепции ЗИ.

51. Нормативная регламентация использования криптографических средств кодирования информации. Указ № 334 от 03.04.95 и последующие нормативно-правовые документы.

52. Работа с кадрами. Прием и увольнение работников. Трудовое законодательство в части приема на работу и увольнения работников.

7.1. Основная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2 http://znanium.com/bookread.php?book=405000

2. Аверченков, В. И. Организационная защита информации [электронный ресурс] : учеб. пособие для вузов / В. И. Аверченков, М. Ю. Рытов. - 3-е изд., стереотип. - М. : ФЛИНТА, 2011. - 184 с. - ISBN 978-5-9765-1272-6 http://znanium.com/bookread.php?book=453862

3. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6 http://znanium.com/bookread.php?book=474838

7.2. Дополнительная литература:

1. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5 http://znanium.com/bookread.php?book=423927

2. Аверченков, В. И. Методы и средства инженерно-технической защиты информации [электронный ресурс] : учеб. пособие / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, Т. Р. Гайнулин, - М. : ФЛИНТА, 2011. - 187 с. - ISBN 978-5-9765-1275-7 http://znanium.com/bookread.php?book=453848

7.3. Интернет-ресурсы:

Кафедра радиофизики КФУ - http://radiosys.ksu.ru/

ОК-1 - http://www.fgosvpo.ru/uploadfiles/fgos/28/20111115114254.pdf

Федеральный государственный образовательный стандарт - http://www.fgosvpo.ru/uploadfiles/fgos/28/20111115114254.pdf

Электронная библиотека КФУ - http://libweb.ksu.ru/ebooks/

Электронно-библиотечная система ZNANIUM - http://znanium.com

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Организационное и правовое 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.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

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.

нет

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 10.03.01 "Информационная безопасность" и профилю подготовки Безопасность компьютерных систем .

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

Рецензент(ы):
Ситников Ю.К. _____
"__" _____ 201 __ г.