АННОТАЦИЯ ДИСЦИПЛИНЫ

«Управление информационной безопасностью »

Дисциплина «Управление информационной безопасностью » является частью программы магистратуры «Комплексные системы информационной безопасности» по направлению «10.04.01 Информационная безопасность».

Цели и задачи дисциплины

Цель - изучение методов и средств управления информационной безопасностью (ИБ) в организации, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ) определенного объекта. Задачи дисциплины: • привитие обучаемым основ культуры обеспечения информационной безопасности; • формирование у обучаемых понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем; • ознакомление обучаемых с основными методами управления информационной безопасностью организаций, объектов и систем; • обучение различным методам реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ конкретной организации..

Изучаемые объекты дисциплины

Понятия, методологии и практические приемы управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии и в организации.

Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		3
1. Проведение учебных занятий (включая проведе-ние текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	54	54
- лекции (Л)	18	18
- лабораторные работы (ЛР)	16	16
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	18	18
- контроль самостоятельной работы (КСР)	2	2
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	90	90
2. Промежуточная аттестация		
Экзамен	36	36
Дифференцированный зачет		
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)	18	18
Общая трудоемкость дисциплины	180	180

Краткое содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
3-й семестр				
Политика информационной безопасности.	2	2	2	10
Понятие политики информационной безопасности. Цели, требования и принципы при разработке и внедрении политики информационной безопасности. Порядок разработки частной политики информационной безопасности. Содержание и жизненный цикл политики информационной безопасности. Ответственность за исполнение политики информационной безопасности				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Управление инцидентами информационной безопасности	2	2	2	10
Нормативная база управления инцидентами информационной безопасности. Сущность процесса управления инцидентами информационной безопасности. Система управления инцидентами информационной безопасности. Этапы процесса управления инцидентами информационной безопасности				
Введение в дисциплину «Управление информационной безопасностью»	2	0	2	10
Цель и задачи изучения дисциплины. Базовая терминология. Система и системный подход. Процесс и процессный подход. Сущность и функции управления. Циклическая модель улучшения процессов. Понятие системы управления. Принципы управления. Цели и задачи управления информационной безопасностью.				
Технические аспекты управления информационной безопасностью	2	2	2	10
Защита от вредоносного программного обеспечения. Управление сетевыми ресурсами. Защита носителей информации. Обмен информацией и программного обеспечения. Вспомогательные операции. Выработка требований по обеспечению информационной безопасности систем. Информационная безопасность приложений, исходных текстов программного обеспечения, исполняемых и системных файлов. Информационная безопасность данных и учетных записей. Информационная безопасность в процессах разработки и сопровождения информационных систем. Защитные меры, связанные с использованием криптографии. Управление конфигурациями, изменениями и обновлениями				
Стандартизация систем и процессов управления информационной безопасностью	2	0	2	10
История развития стандартизации в области ИБ. Основные стандарты и методологии по управлению информационной безопасностью. Серия стандартов ISO 27000. Стандарты банковской системы Российской Федерации СТО БР ИББС. Рекомендации в области стандартизации. Стандарты на отдельные процессы управления				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
информационной безопасностью и оценку безопасности информационных технологий: ISO\IEC 13335, ISO\IEC 15408, ISO\IEC 18045, BS 25999/25777, ГОСТ Р 53647. Стандарты CoBiT. Преимущества и недостатки применения основных стандартов в области информационной безопасности.				
Технические аспекты управления информационной безопасностью	2	2	2	10
Политика в отношении логического доступа. Управление доступом пользователей. Обязанности пользователя при доступе к активам. Управление сетевым доступом. Управление доступом к операционной системе. Управление доступом к приложениям. Работа с мобильными устройствами в дистанционном режиме. Доступ к средствам обработки информации сторонних лиц и/или организаций.				
Управление и система управления информационной безопасностью	2	2	2	10
Деятельность по обеспечению информационной безопасностью организации. Основные методы управления информационной безопасностью. Управление информационной безопасностью информационно-телекоммуникационными технологиями организации. Система управления информационной безопасностью организации (СУИБ). Процессный подход в рамках управления информационной безопасностью организации. Работа с процессами СУИБ организацией. Стратегии построения и внедрения процессов СУИБ организацией. Совершенствование СУИБ				
Оценка и обработка рисков информационной безопасности	2	2	2	10
Нормативное обеспечение управления рисками информационной безопасности. Основы рисковой деятельности. Сущность и роль управления рисками информационной безопасности. Порядок оценки рисков информационной безопасности. Методы оценки рисков информационной безопасности. Процесс обработки рисков как этап управления рисками информационной безопасности. Варианты обработки рисков. Принятие, коммуникация, мониторинг и				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
пересмотр рисков информационной безопасности. Обеспечение управления рисками информационной безопасности				
Сущность аудита информационной безопасности	2	4	2	10
Назначение и цели аудита информационной безопасности. Виды аудита. Принципы проведения аудита информационной безопасности. Управление программой аудита информационной безопасности. Требования к аудитору информационной безопасности и оценка его работы. Измерение эффективности СУИБ. Метрики эффективности. Этапы и организация работ по проведению аудита информационной безопасности. Области и критерии аудита информационной безопасности. Анализ документации. Интервьюирование персонала и непосредственное наблюдение за деятельностью. Подготовку и утверждение отчета по аудиту информационной безопасности. Разработка мероприятий и проработка решений по устранению выявленных нарушений				
ИТОГО по 3-му семестру	18	16	18	90
ИТОГО по дисциплине	18	16	18	90