

## АННОТАЦИЯ ДИСЦИПЛИНЫ

### «Прогнозирование рисков информационной безопасности»

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

#### **Цели и задачи дисциплины**

Цель - освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе технологии прогнозирования, оценки и обработки рисков информационной безопасности. Задачи дисциплины: • изучение основных положений, понятий и категорий теоретических основ управления рисками информационной безопасности; • изучение предпосылок для управления информационными рисками; • изучение основных требований по управлению рисками информационной безопасности; • изучение состава системы управления информационными рисками; • формирование умений оценки рисков информационной безопасности; • формирование умений обработки рисков информационной безопасности; • формирование навыков по оценке угроз безопасности информации в технологии оценки рисков; • формирование навыков подбора инструментальных средств для управления рисками информационной безопасности..

#### **Изучаемые объекты дисциплины**

• современные информационные риски и их особенности; • стандарты управления рисками; • стандарты в области управления рисками информационной безопасности; • система управления информационными рисками; • порядок оценки рисков информационной безопасности; • анализ угроз и уязвимостей; • профиль и жизненный цикл угрозы; • описание угроз безопасности; • способы классификации угроз; • уязвимости информационной безопасности; • идентификация организационных и технических уязвимостей; • оценка угроз и уязвимостей; • определение величины риска; • процесс и способы обработки рисков; • инструментальные средства для управления рисками..

### Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		3	
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме:	54	54	
1.1. Контактная аудиторная работа, из них:			
- лекции (Л)	18	18	
- лабораторные работы (ЛР)	32	32	
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)			
- контроль самостоятельной работы (КСР)	4	4	
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	126	126	
2. Промежуточная аттестация			
Экзамен	36	36	
Дифференцированный зачет			
Зачет			
Курсовой проект (КП)			
Курсовая работа (КР)			
Общая трудоемкость дисциплины	216	216	

### 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				
Оценка угроз безопасности информации в технологии оценки рисков	2	4	0	14
Анализ угроз и уязвимостей. Профиль и жизненный цикл угрозы. Описание угроз безопасности. Способы классификации угроз. Уязвимости информационной безопасности. Идентификация организационных уязвимостей. Идентификация технических уязвимостей. Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Пример оценки риска. Отчет об оценке рисков.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Обработка рисков информационной безопасности	2	4	0	14
Процесс обработки рисков. Способы обработки риска. Принятие риска. Уменьшение риска. Передача риска. Избегание риска. Оценка возврата инвестиций в информационную безопасность. Принятие решения по обработке риска. План обработки рисков. Декларация о применимости механизмов контроля. Профили рисков информационной безопасности.				
Инструментальные средства для управления рисками	2	4	0	14
Актуальность программного сопровождения процедуры оценки рисков. Выбор программного обеспечения для оценки рисков. Общие недостатки и ограничения коммерческих программных продуктов. Обзор методов и инструментальных средств управления рисками: OCTAVE, CRAMM, RiskWatch, CORBA, RA2 the art of risk, vsRisk, Proteus Enterprise.				
Внедрение системы прогнозирования и управления рисками информационной безопасности	2	4	0	14
Особенности внедрения системы управления информационными рисками (СУИР). Документация. Начальные условия для внедрения СУИР. Организационная структура управления рисками. Обучение членов экспертной группы. Проведение полной оценки рисков по всем активам. Жизненный цикл управления рисками.				
Основные требования по управлению рисками информационной безопасности	2	4	0	14
Стандарты в области управления рисками информационной безопасности. Понятие риска. Оценка риска. Количественное определение величины риска. Качественное определение величины риска. Информационная составляющая бизнес - рисков. Активы организации как ключевые факторы риска. Подходы к управлению рисками. Уровни зрелости бизнеса в отношении рисков. Анализ факторов риска. Методика оценки рисков приватности,				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
включая персональные данные				
Система управления информационными рисками	2	4	0	14
Преимущества системного подхода к управлению рисками. Структура документации по управлению рисками. Политика и контекст управления рисками. Структура системы управления рисками. Процессная модель управления рисками. Непрерывная деятельность по управлению рисками. Сопровождение и мониторинг механизмов безопасности. Анализ со стороны руководства. Пересмотр и переоценка риска. Взаимосвязь процессов аудита и управления рисками. Управление документами и записями. Корректирующие и превентив-ные меры. Коммуникация рисков. Аутсорсинг процессов управления рисками. Распреде-ние ответственности за управление рисками. Требования к риск-менеджеру. Требования к эксперту по оценке рисков.				
Предпосылки для управления информационными рисками	2	4	0	14
Современные информационные риски и их особенности. Кибертерроризм. Риски промышленных систем. Риски утечки информации. Риски электронных расчетов. Стандарты управ-ления рисками. Государственное регулирование. Оценка рисков как основа корпоративного управления.				
Введение в дисциплину	2	0	0	14
Основные понятия, термины и определения. Предмет и задачи дисциплины. Цели и задачи курса и его место в подготовке магистров. Особенности формирования терминологии науч-ной дисциплины. Взаимосвязь курса с другими дисциплинами учебного плана. Методические материалы. Периодические издания. Обязательная и дополнительная литература.				
Оценка рисков информационной безопасности	2	4	0	14
Идентификация активов. Описание бизнес-процессов. Идентификация требований безопасности. Реестр требований				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
безопасности. Требования законодательства и нормативной базы. Контрактные обязательства. Требования бизнеса. Определение ценности активов. Критерии оценки ущерба. Таблица ценности активов. Особенности интервьюирования бизнес-пользователей. Определение приоритетов аварийного восстановления.				
ИТОГО по 3-му семестру	18	32	0	126
ИТОГО по дисциплине	18	32	0	126