Аннотация рабочей программы дисциплины

по направлению 09.03.02 Информационные системы и технологии

,

профиль: Безопасность информационных систем

Методы и технологии расследования инцидентов информационной безопасности

Наименование разделов и тем дисциплины:

№	Содержание раздела
Раздел 1	Знакомство с ГОСТ Р ИСО/МЭК ТО 18044-2007. Главы ГОСТа 1-3: Введение, Область применения, Нормативные ссылки, Термины и определения, Общие положения
Раздел 2	Оформление документов по расследованию инцидента информационной безопасности. Привлечение нарушителя к дисциплинарной ответственности. Взаимодействие с юридической службой и руководителем нарушителя. Виды взысканий, порядок наложения и снятия дисциплинарного взыскания.
Раздел 3	Понятие менеджмента инцидентов информационной безопасности. Этапы менеджмента инцидентов информационной безопасности. Подготовка и планирование системы менеджмента. Использование системы менеджмента. Анализ и совершенствование системы менеджмента инцидентов информационной безопасности.
Раздел 4	Создание группы расследования инцидентов информационной безопасности. Документация системы менеджмента инцидентов информационной безопасности. Извлечение уроков из инцидентов информационной безопасности. Тенденции, проблемные области, выявляемые в ходе анализа инцидентов информационной безопасности. База инцидентов информационной безопасности. Формы сообщений об инцидентах информационной безопасности. Особенности практического использования системы менеджмента инцидентов информационной безопасности в организации.
Раздел 5	Международные стандарты в области информационной безопасности и лучшие практики по управлению инцидентами информационной безопасности. Классификация инцидентов информационной безопасности.
Раздел 6	Проведение расследований инцидентов информационной безопасности: назначение руководителя расследования, сбор свидетельств возникновения инцидентов, обеспечение их сохранности. Планирование расследования. Алгоритм действий работников группы реагирования при возникновении инцидентов информационной безопасности. Выявление нарушителя, установление причин и мотивов инцидента информационной безопасности, опрос нарушителя и свидетелей инцидента, сбор объяснений по факту инцидента информационной безопасности.
Раздел 7	Возможные последствия инцидентов информационной безопасности. Понятие ущерба. Виды ущерба: прямой, косвенный, репутационный. Оценка ущерба от инцидента информационной безопасности. Основные предпосылки возникновения инцидентов информационной безопасности в организации. Категории нарушителей информационной безопасности: внутренние и внешние. Модель

	нарушителя информационной безопасности. Основные мотивы совершения инцидентов информационной безопасности.