Аннотация к рабочей программе по дисциплине «Менеджмент инцидентов информационной безопасности»

1. Цели освоения дисциплины

Целями изучения дисциплины «Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления» являются: - выработка навыков по обнаружению, оповещению об инцидентах информационной безопасности и их оценки; - обучить реагировать на инциденты информационной безопасности, включая активизацию соответствующих защитных мер для предотвращения, уменьшения последствий и восстановления после негативных воздействий; - анализ инцидентов информационной безопасности, введение превентивных защитных мер и улучшению общего подхода к менеджменту инцидентов информационной безопасности. Задачами «Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления» являются формирование у студентов знаний позволяющих: - обнаруживать события информационной безопасности и эффективно их обрабатывать, также определять относятся или не относятся данные события к инцидентам информационной безопасности; - давать оценку инцидентам информационной безопасности; - минимизировать воздействие инцидентов информационной безопасности на защищенные автоматизированные системы управления.

2. Место дисцплины в структуре ООП

Б1.В.ДВ.03.02

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций по данному направлению:

ПК-22 - способностью анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности;

В результате освоения дисциплины обучающийся должен

знать:

- нормативные правовые акты в области обеспечения; оценивать основные процессы управления информационной безопасностью защищенных автоматизированных систем управления - критерии оценки инцидентов информационной безопасности; - классификацию инцидентов - основные службы безопасности, стандарт ISO 17799:2000, политику информационной безопасности

уметь:

- пользоваться государственными и международными стандартами по менеджменту инцидентов информационной безопасности защищенных автоматизированных систем управления - применять на практике технологии и средства защиты для минимизации ущерба от инцидентов информационной безопасности

иметь навыки и (или) опыт деятельности:

- организационными и техническими средствами для выявления и устранения инцидентов информационной безопасности защищенных автоматизированных систем - информацией о состоянии защищенной автоматизированной системы - оценкой соответствия средств защиты информации подсистемам обеспечения информационной безопасности защищенных автоматизированных систем управления нормативным требованиям по защите информации

4. Общая трудоемкость дисциплины

180(в часах) 5 з.е.

5. Формы контроля

зачет (9 семестр)