АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ

(название дисциплины)

10.04.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

(код направления (специальности) подготовки)

1,2

(семестр)

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

- «Информационно-аналитические системы безопасности» являются обеспечение подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.04.01 «Информационная безопасность». Целью освоения дисциплины является ознакомление магистров с информационно – аналитическими системами безопасности, с типовой структурой корпоративной информационной системы, с методиками анализа и активного аудита безопасности такого класса систем, а также с наиболее вероятными угрозами информационной безопасности в корпоративной информационно-вычислительной среде.
- Дисциплина обеспечивает необходимые знания для организации и управления службой безопасности на предприятии, комплектования ее профессионально подготовленными кадрами.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

- Данная дисциплина относится к дисциплинам по выбору вариативной части Блока Б1 (код Б1.В.ДВ.3). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ.
- Дисциплина изучается на 2 курсе, в 3 семестре требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по направлению 10.04.01 «Информационная безопасность» по курсам «Анализ и моделирование информационно-телекоммуникационных сетей», «Методы и средства защиты объектов информатизации», «Методология информационной безопасности», «Оценка и контроль обеспечения информационной безопасности», «Методы информационно-аналитической работы». Кроме того, требования к «входным» знаниям, умениям и готовностям обучающегося определяются требованиями к уровню подготовки выпускника бакалавриата при освоении курсов «Защита информации в корпоративных информационных системах» или аналогичных, в соответствии с программой подготовки бакалавров в следующих или смежных областях знаний: -информационная безопасность; -энергетика, энергетическое машиностроение и электротехника; -авиационная и ракетно-космическая техника; -фотоника, приборостроение, -оптические и биотехнические системы и технологии; -электронная техника, радиотехника и связь; -автоматика и управление; -информатика и вычислительная техника; -физико-технические науки и технологии; -управление в технических системах.
- Курс тесно взаимосвязан с другими дисциплинами. Он может быть полезен для изучения таких дисциплин как «Управление информационной безопасностью», «Защищённые информационные системы» и т.д.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины студент должен обладать следующими общекультурными и профессиональными компетенциями:

- ПК-8 – способностью обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;
- ПК-9 – способностью проводить аудит информационной безопасности информационных систем и объектов информатизации.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

- Основные направления обеспечения безопасности объекта.
- Концептуальная модель безопасности предприятия (фирмы).
- Информационно-аналитическое обеспечение предпринимательской деятельности и безопасности бизнеса.
- Построение системы защиты коммерческой тайны на предприятии.
- Персонал и безопасность предприятия.
- Психологическое обеспечение безопасности предпринимательской деятельности.

- Финансовая составляющая безопасности предприятия.
- Криминальные сообщества, недобросовестная конкуренция и безопасность предприятия.
- Методические основы обеспечения информационной безопасности объекта. План защиты объекта и его реализация
- Всего
- Конкурентная разведка. Виды и технологии конкурентной разведки.
- Нормативные документы, регламентирующие деятельность службы конкурентной разведки на предприятии.
- Методика сбора информации о юридическом лице. Методика сбора информации о физическом лице.
- Организация защиты информации на предприятии. Правовое обеспечение защиты информации. Организационные мероприятия по защите информации.
- Инженерно-техническая защита информации. Программно-аппаратные средства защиты информации.
- Элементы контрразведывательной деятельности в работе службы безопасности предприятия.
- Инсайдеры. Методы борьбы с инсайдерами.
- Интернет и компьютеры как инструменты конкурентной разведки.
- Ситуационные центры. Технологии, используемые в информационно-аналитических системах безопасности (управление знаниями, интеллектуальный анализ данных, обнаружение знаний в базах данных и т.д.).

Составитель: зав. кафедрой ИЗИ д.т.н., Монахов М.Ю.

должность, ФИО, подпись

Заведующий кафедрой ИЗИ М.Ю. Монахов

ФИО, подпись

Директор института ИТР А.А. Галкин

ФИО, подпись

Дата, Печать института (факультета)