

### **Аннотация**

**рабочей программы учебной дисциплины Б1.Б.20 «Безопасность информационно-аналитических систем»**

**специальности 10.05.04 Информационно-аналитические системы безопасности**

**специализация №2 «Информационная безопасность финансовых и экономических структур»**

**Цели изучения курса:** освоение дисциплинарных компетенций, связанных с раскрытием технологий интеллектуального анализа больших информационных массивов посредством помощью информационно-аналитических систем.

#### **Задачи курса:**

- изучение основных положений, понятий и категорий, связанных с информационно-аналитическими системами безопасности

- изучение основных принципов, связанных с организацией конкурентной(деловой) разведки, ее целей и задач, моделей конкурентной среды, методик сбора информации о юридических и физических лицах

- изучение правовых основ и принципов деловой разведки, нормативных документов, регламентирующих деятельность соответствующих служб,

- изучение основных подходов к выполнению интеллектуального анализа больших массивов данных посредством современных информационных технологий

- формирование умений, связанных с стандартизованным представлением данных и оформлением аналитических результатов, формулированием умозаключений и выводов об объектах анализа, оформлением результатов анализа в виде аналитических записок и отчетов; умений по сбору и классификации информации полученной в ходе деловой разведки, ее оценке и структурированию

- формирование навыков противодействия злоумышленной активности на предприятиях путем организации соответствующих подразделений, а также с использованием современных информационно-вычислительных средств и систем

#### **Основные блоки и темы дисциплины:**

Тема 1. Объект анализа в информационно-аналитической деятельности

Тема 2. Представление данных и оформление аналитических результатов

Тема 3. Конкурентная (деловая) разведка

Тема 4. Разведывательные циклы деловой разведки

Тема 5. Организация противодействия злоумышленной деятельности на предприятии

Тема 6. Программные технологии в системе информационно-аналитического обеспечения безопасности.

**Учебная дисциплина «Безопасность информационно-аналитических систем» входит в перечень дисциплин базовой части цикла ОП.**

В результате изучения дисциплины специалист должен обладать следующими компетенциями:

#### **Знать:**

основные положения, понятия и категории, связанные с информационно-аналитическими системами безопасности. (ОПК-7);

правовые основы и принципы деловой разведки, нормативные документы, регламентирующие деятельность соответствующих служб; основные принципы противодействия инсайдерским угрозам на предприятии; теоретические основы исследования информационных процессов предприятий, организаций, их классификацию; угрозы безопасности информации, модели нарушителя информационных систем, возможности проникновения нарушителя в информационную систему. (ПК-9);

основные принципы противодействия инсайдерским угрозам на предприятии. (ПК-10)

#### **Уметь:**

осуществлять стандартизованное представление данных об объекте и оформлять полученные аналитические результаты. (ОПК-7);

организовывать противодействие злоумышленной активности на предприятиях путем создание соответствующих подразделений, а также с использованием современных информационно-вычислительных средств и систем; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; определять виды и формы информации, подверженной угрозам, классифицировать и систематизировать информационные массивы предприятий и организаций по совокупности признаков, определять возможные методы и пути реализации угроз. (ПК-9);

организовывать противодействие злоумышленной активности на предприятиях путем создание соответствующих подразделений, а также с использованием современных информационно-вычислительных средств и систем; применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. (ПК-10)

**Владеть:**

навыками противодействия злоумышленной активности, связанной с инсайдерскими угрозами на предприятиях. (ОПК-7);

навыками противодействия злоумышленной активности, связанной с инсайдерскими угрозами на предприятиях; навыками организации охраны объектов информатизации и обеспечения режима секретности, организации и управления деятельностью службы защиты информации на предприятии; навыками разработки моделей информационных процессов предприятий и организаций, оценки уязвимости информации различных видов и форм, выбора технологий, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых информационных систем. (ПК-9);

навыками организации охраны объектов информатизации и обеспечения режима секретности, организации и управления деятельностью службы защиты информации на предприятии. (ПК-10).

Дисциплина «Безопасность информационно-аналитических систем» изучается посредством лекций, все разделы программы закрепляются лабораторными занятиями, выполнением контрольных работ, самостоятельной работы над учебной и научно-технической литературой и завершается зачетом.

**Общая трудоемкость дисциплины** составляет 4 зачетные единицы (144 часов).

**Вид промежуточной аттестации:** зачет.

Разработчик

*Сапиев А.З.*

А.З. Сапиев

Зав. выпускающей кафедрой



В.Ю. Чундышко