Тренинг: «Информационно-аналитическая работа службы безопасности предприятия. Профессиональные секреты и «продвинутые» методы. *Третий уровень трехэтапного цикла обучения аналитиков подразделений безопасности».*

Продолжительность обучения: 2 дня, 16 академических часов.

Категория обучаемых: Руководители, специалисты и аналитики служб безопасности, а также сотрудники компаний, связанные с решением информационно-аналитических задач в сфере обеспечения безопасности бизнеса.

Целевая установка: Формирование «продвинутых» нестандартных навыков поиска и анализа информации с использование источников различных категорий, и освоение методики выявления индикаторов потерь и хищений и проведения расследований умышленных противоправных действий на примерах реальных бизнес-процессов.

Краткая аннотация. В рамках интенсивного двухдневного обучения слушатели осваивают наиболее сложные и высокоэффективные приёмы и инструменты поиска и анализа информации и на реальных примерах изучают методика предупреждения, выявления и расследования потерь и хищений в общей системе обеспечения экономической безопасности компании.

Содержание программы:

Тема 1. Создание собственной базы данных службы безопасности (необходимые ИТ-компетенции сотрудника службы безопасности).

- Построение базы данных для работы службы безопасности с «чувствительной» информацией на платформе Microsoft Excel без привлечения ИТ-специалистов.
- Подключение внутренних и внешних источников к собственной базе данных.
- «Продвинутые» варианты доступа и загрузки при работе с внутрикорпоративными источниками информации.

Тема 2. «Продвинутые» приемы информационно-аналитической работы службы безопасности (профессиональные секреты в работе службы безопасности).

- Приемы выявления внешнего коррупционного окружения, параллельного бизнеса и других скрытых каналов потерь и хищений на предприятии, на основе консолидированного анализа внешних и внутренних источников.

- Использование электронной переписки пользователей для решения задач их поиска, идентификации и деанонимизации в социальных сетях и других ресурсах сети Интернет.
- Практические примеры установления авторов публикаций, направленных на причинение ущерба деловой репутации предприятия.
- Использование фото- и видеоизображений из внешних и внутренних источников информации для решения задач поиска неофициальных связей между людьми, определения географического местоположения объектов, выявления значимых событий и объектов, автоматической классификации фото- и видеоизображений.
- Самостоятельное решение практических задач под руководством преподавателя.

Тема 3. Аналитические методы и практические приемы работы с финансовой информацией из внутренних и внешних источников (необходимые бухгалтерские и аудиторские компетенции сотрудника службы безопасности).

- Анализ финансового состояния и надежности предприятия по данным финансовой отчетности.
- Скоринговые модели оценки финансового состояния и надежности предприятия в работе службы безопасности.
- Подключение в режиме чтения к базе данных бухгалтерии и выгрузка информации, необходимой для предупреждения и выявления потерь и хищений.
- Практические приемы выявления фактов злоупотреблений и мошенничества на основе анализа регистров бухгалтерского учета.
- Самостоятельное решение практических задач под руководством преподавателя.

Тема 4. Практические приемы визуализации данных в работе службы безопасности.

- Оперативный, аналитический и стратегический отчет в работе службы безопасности.
- Виды графиков и диаграмм, методика их выбора и построения.
- Создание отчетов для управления безопасностью на предприятии.
- Создание отчета для первого лица в форме информационной панели (дашборда).
- Самостоятельное решение практических задач под руководством преподавателя.

Деловая игра «Выявление фактов злоупотреблений и мошенничества и поиск скрытых источников менеджмента предприятия».

Заключение. Тестирование полученных практических навыков и построение личной карты уровня профессиональных компетенций.