САНКТ-ПЕТЕРБУРГСКАЯ АКАДЕМИЯ БЕЗОПАСНОСТИ

АНО ДПО «Санкт-Петербургская академия безопасности»
194044, Санкт-Петербург, Лесной пр., д. 20, корп. 15
Тел.: (812) 603-28-74, e-mail: info@nsab.ru, www.nsab.ru

Программа повышения квалификации

«Основные аспекты обеспечения корпоративной (внутренней) безопасности»

Продолжительность: 5 дней (34 академических часа).

Категории слушателей:

- директоры по безопасности, заместители директоров по безопасности;
- начальники отделов (служб) экономической безопасности (ЭБ);
- главные (ведущие) специалисты подразделений экономической безопасности.

Содержание программы

1. Основные аспекты внутренней безопасности.

1.1. Система внутренней безопасности, субъекты системы, объекты системы.
1.2. Цели и задачи, решаемые системой внутренней безопасности предприятий.
1.3. Внутренние и внешние угрозы в системе внутренней безопасности предприятий.
1.4. Бизнес-процессы системы внутренней безопасности предприятий.

2. Противодействие мошенничеству.

2.1. Корпоративное мошенничество и иные преступления против собственности.
- Понятие и признаки мошенничества.
- Виды, основные приемы и методы корпоративного мошенничества.

2.2. Портрет мошенника.
- Мошенники и их мотивация.
- Понятие треугольника мошенничества.

2.3. Модели мошеннических операций.
- Признаки корпоративного мошенничества со стороны различных категорий персонала.

2.4. Меры по предупреждению корпоративного мошенничества.

3. Организация работы службы безопасности по организации охранных мероприятий.

3.1. Организация пропускного и внутриобъектового режима.
3.2. Участие в комиссиях по инвентаризации товарно-материальных ценностей.
3.3. Контроль за работой охранных структур.
3.4. Безопасность служебных помещений и сотрудников предприятия.
3.5. Обеспечение безопасности проведения корпоративных мероприятий.

4. Работа службы внутреннего контроля (семинар).

4.1. Специфика проявления внутренних угроз предприятиям.
4.2. Обсуждение методов и средств обеспечения внутренней (собственной) безопасности, используемых на предприятиях.

5. Основные направления обеспечения кадровой безопасности предприятий.

5.1. Кадровая безопасность в системе обеспечения безопасности предприятия.
5.2. Задачи службы безопасности в процессе подбора сотрудников.
5.2.1. Основные мероприятия, проводимые при приеме сотрудников:
- оформление согласия на сбор и обработку персональных данных;
- изучение профиля кандидата путем анализа представленных им документов (резюме, анкета, автобиография), посредством получения рекомендаций с предыдущих мест работы и просмотра социальных сетей;

- признаки неблагонадежности у претендентов на работу, применение графоанализа при приеме на работу.

5.2.2. Особенности приема отдельных категорий персонала, связанные с материальной ответственностью.

5.2.3. Юридическое оформление отказа в приеме на работу.

5.3. Методы изучения и проверки кандидата на работу и работающего персонала**.**

5.3.1. Основные аспекты использования полиграфа в решении задач обеспечения экономической безопасности предприятия.

- правовые основы использования полиграфа;
- основные возможности полиграфа;
- порядок использования полиграфа;
- практическая демонстрация использования полиграфа.

5.3.2. Методика проведения входной беседы с кандидатами на работу и работающим персоналом в целях обеспечения безопасности предприятия.

5.3.3. Основы профайлинга при проведении скрининговых проверок.

5.3.3.1. Составление психологического портрета на основе анализа вербальных и невербальных признаков.

5.3.3.2. Методики оценки и прогнозирования факторов риска кандидатов различного психологического профиля.

5.4. Задачи службы безопасности в процессе увольнения сотрудников.

5.4.1. Основные мероприятия, проводимые при увольнении сотрудников:

- правила проведения индивидуальных бесед с увольняющимися сотрудниками;
- факторы «безопасного увольнения»;
- обеспечение лояльности увольняющихся сотрудников;
- определение истинных причин увольнения сотрудника.

5.4.2. Процессуальное оформление увольнения сотрудников, «представляющих опасность».

5.4.3. Правила работы с увольняющимися сотрудниками, имевшими доступ к конфиденциальной информации.

6. Работа с информационными источниками.

6.1. Основы привлечения информационных источников.

6.2. Порядок привлечения информационных источников.

6.3. Организация обучения и инструктажей информационных источников.

7. Персонал предприятия как фактор риска утечки защищаемой информации.

7.1. Организация обеспечения информационной безопасности:

- информационные ресурсы организации;
- угрозы информационной безопасности предприятия, исходящие от персонала;
- политика информационной безопасности предприятия;
- ответственность за нарушения требований, правил и мер защиты информации;
- обеспечение работы персонала с соблюдением мер информационной безопасности;

7.2. Технические и программные средства обеспечения информационной безопасности предприятия.

7.3. Основы использования DLP-систем.

- Возможности DLP-систем для контроля информационных потоков на предприятии, электронной переписки, нарушения политики безопасности.
- Проведение расследований и предупреждение противоправных действий с использованием возможностей DLP-систем.

7.4. Мониторинг профилей персонала предприятия в социальных сетях и сети Интернет.

7.5. Правовые основы и технические методы работы службы безопасности по выявлению, пресечению и предупреждению со стороны персонала действий, наносящих экономический ущерб предприятию.

8. Проведение внутренних служебных расследований по выявленным нарушениям.

8.1. Алгоритм проведения на предприятии служебных расследований (разбирательств) по фактам нарушений со стороны сотрудников предприятия.

8.2. Особенности служебного расследования в случаях причинения материального ущерба имуществу организации.

8.3. Подготовка заключений по результатам проведенных разбирательств.

8.4. Взаимодействие с правоохранительными органами в рамках обеспечения внутренней безопасности.

9. Итоговая аттестация.

При успешном прохождении итоговой аттестации по данной программе слушателям выдается **Удостоверение о повышении квалификации.**