Бауманский учебный центр «Специалист»

Программа курса Руководитель службы информационной безопасности и защиты от хакерских атак

Код курса: **CEH4**

Тема	Ак. часов

Модуль 1. Политики, юридические аспекты и соответствие стандартам
• Основные определения
• Программа управления информационной безопасностью
  ◦ Политика безопасности
  ◦ Роли и зоны ответственности
  ◦ Стандарты безопасности. Рекомендации, фреймворки
  ◦ Управление рисками
  ◦ Техническая архитектура системы безопасности
  ◦ Классификация активов и управление
  ◦ Бизнес-устойчивость
  ◦ Тренинги и осведомленность
• Законы, нормативы и руководства информационной безопасности
  ◦ Законы и нормативно-правовые акты широкого применения
  ◦ Отраслевые нормативно-правовые акты
  ◦ Ключевые нормативно-правовые акты
  ◦ Международные законы
• Законы, защищающие частную жизнь гражданина
  ◦ Законы о неправомерном раскрытии информации
  ◦ Международные законы о частной жизни
	8

Модуль 2. Контроль и аудит системы управления • Проектирование, развертывание и управление защитными мерами в соответствии с целями бизнеса, границами риска, политиками и стандартами • Инвентаризация рисков информационной безопасности • Обработка риска • Остаточный риск • Принятие риска • Управление риском • Бизнес-цели • Границы риска • Политики и стандарты • Типы мер безопасности • Внедрение системы обеспечения управления • COBIT и BAI • ISO 27001/27002 • Автоматизированные меры безопасности • Процесс аудита управления • Заключение	**8**

Модуль 3. Проекты, технологии и операции
 	
• Роль CISO
  ◦ Оценка
  ◦ Планирование
  ◦ Проектирование
  ◦ Исполнение
  ◦ Метрики и отчеты
• Проекты информационной безопасности
  ◦ Соответствие целям бизнеса
  ◦ Идентификация акционеров проекта
  ◦ Соответствие границам риска
  ◦ Практические рекомендации выполнения проекта информационной безопасности
• Управление безопасностью операций
  ◦ Функции и навыки сотрудников
  ◦ Планирование коммуникаций
  ◦ Управление поставщиками
  ◦ Учет
  ◦ Интеграция требований безопасности в другие процессы
	8

Модуль 4. Ключевые концепции и технологии защиты информации • Управление доступом • Физическая безопасность • Восстановление после сбоев • Сетевая безопасность • Управление угрозами и уязвимостями • Безопасность приложений • Безопасность операционных систем • Шифрование • Расследование инцидентов и реагирование на инциденты	**8**
Модуль 5. Стратегическое планирование и финансы • Введение в стратегическое планирование • Соответствие целям бизнеса и границы риска • Взаимосвязь политик, соответствий и конфиденциальности • Руководящая роль • Архитектура информационной безопасности предприятия • Новые тенденции в безопасности • Защита данных • Сертификация систем и процесс аккредитации • Планирование ресурсов • Планирование финансов • Контракт на поставку • Управление поставщиками • Запрос предложений • Интеграция требований безопасности в контрактные соглашения • Регламент оказания услуг • Соглашение об уровне обслуживания	**8**
Аудиторная нагрузка в классе с преподавателем	**40 ак.ч. + 40 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru