АУДИТ, УПРАВЛЕНИЕ РИСКАМИ И ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель – углубленное ознакомление и изучение вопросов проведения аудита, управления рисками и инцидентами информационной безопасности. Выпускники курса получают государственные документы о повышении квалификации в области информационной безопасности.

В курсе обобщен и систематизирован материал лучших практик по проведению аудита, управлению рисками и инцидентами информационной безопасности, представленный в международных, национальных и фирменных стандартах. Особое внимание уделяется методологическому обеспечению рассматриваемых вопросов. Подробно рассматриваются вопросы организации работ при проведении аудита, анализа рисков и расследования компьютерных инцидентов.

Аудитория

- руководители подразделений технической защиты информации, ответственные за состояние информационной безопасности и организацию работ по созданию комплексных систем защиты информации;
- аналитики по вопросам компьютерной безопасности, ответственные за анализ состояния информационной безопасности, определение требований к защищенности ресурсов автоматизированных систем и путей обеспечения их защиты;
- специалисты, ответственные за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам защиты информации;
- менеджеры, ответственные за работу с персоналом по вопросам обеспечения информационной безопасности.

Требуемая предварительная подготовка слушателей:

- общие представления об информационных системах, правовых, организационных и технических аспектах обеспечения информационной безопасности компьютерных систем;
- базовые знания по IP-сетям, основным протоколам и службам стека TCP/IP;
- навыки работы в ОС Windows или Linux;
- прослушать один из курсов:
- «Безопасность информационных технологий»;
- «Безопасность корпоративных информационных сетей»;
- «Основы безопасности информационных технологий».

Форма обучения – очная (дневная)

Обучение проводится отделом образовательных услуг республиканского унитарного предприятия «Национальный центр обмена трафиком» по адресу: г. Минск, ул. К.Цеткин, 24, в соответствии с графиком учебного процесса

Программа рассчитана на 76 часов учебных занятий.

Учебно-тематический план

№ п/п	**Название тем**
	Система управления информационной безопасностью
1.1	Управление информационной безопасностью
1.2	Система управления информационной безопасностью (СУИБ). Основные понятия, терминология, определение области действия СУИБ. Модель зрелости управления процессами, мониторинг и отчетность
1.3	Правовое обеспечение процессов информатизации и информационной безопасности
1.4	Безопасность технологий виртуализации
1.5	Требования по информационной безопасности.
	Аудит информационной безопасности
2.1	Понятие аудита безопасности, цели и задачи его проведения. Актуальность аудита, основные
2.2	Методики и стандарты, используемые при проведении аудита безопасности информационных систем
2.3	Планирование аудита безопасности информационных систем. Управление процессом аудита. Примеры аудита ИБ.
	Управление информационными рисками
3.1	Управление информационными рисками
3.2	Выявление уязвимостей и угроз информационных ресурсов. Определение параметров угроз. Методология анализа и оценки информационных рисков
3.3	Планы снижения/контроля информационных рисков, корректирующие и превентивные действия, контроль выполнения принятых мер

	Управление инцидентами информационной безопасности.
4.1	Основные понятия и классификация компьютерных инцидентов (КИ). Основные
4.2	Расследование КИ в РБ и за рубежом
4.3	Действия в случае возникновения КИ