

## ЗАЩИТА ИНФОРМАЦИИ В КОРПОРАТИВНЫХ СИСТЕМАХ

**Цель** – углубленное практическое изучение вопросов сетевой компьютерной безопасности, построения и эксплуатации защищенных информационных систем.

Материалы посвящены вопросам создания и эксплуатации защищенных информационных систем. Подробно рассматриваются все этапы создания и ввода в эксплуатацию защищенных систем, а также состав работ при эксплуатации и администрировании защищенных систем. Особое внимание уделяется технологии обеспечения информационной безопасности, рациональному распределению функций и организации эффективного взаимодействия по вопросам защиты информации всех подразделений и сотрудников, использующих и обеспечивающих функционирование автоматизированных систем.

Рассматриваются возможности различных видов программно-аппаратных средств защиты и даются рекомендации по выбору рациональных вариантов решений и их эффективному применению для противодействия угрозам безопасности.

### **Аудитория**

- эксперты и аналитики по вопросам компьютерной безопасности, ответственные за анализ состояния информационной безопасности, определение требований к защищенности сетевых ресурсов, выбор путей и средств обеспечения защиты сетей;
- системные и сетевые администраторы, ответственные за безопасность компьютерных сетей организаций, обоснованный выбор и эффективную эксплуатацию средств защиты и средств анализа (контроля) защищенности сетей;
- руководители подразделений технической защиты информации, ответственные за состояние информационной безопасности и организацию работ по созданию комплексных систем защиты информационных технологий;
- администраторы 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
	<b>Меры по обеспечению безопасности информации в информационных системах.</b>
1.1	Введение в проблему безопасных информационных систем (ИС)
1.2	Теоретические основы защиты информации
1.3	Организационно-методическое обеспечение системы безопасности в ИС
1.4	Обеспечение безопасности информации в ИС
	<b>Системы безопасности в информационных системах.</b>
2.1	Подсистемы безопасности операционных систем
2.2	Криптографические методы защиты информации
2.3	Аппаратно-программные средства защиты информации
2.4	Защищенные виртуальные частные сети VPN
	<b>Аудит защищённой ИС. Управление рисками.</b>
3.1	Аудит защищённой ИС. Управление рисками.
	<b>Создание и эксплуатация защищенных информационных систем.</b>

4.1	Организация защиты информации в системах электронного документооборота
4.2	Проектирование защищённых корпоративных систем
4.3	Аттестация систем защиты информации корпоративных систем
4.4	Эксплуатации защищенных ИС. Администрирование безопасности информации ИС
4.5	Оценка затрат на информационную безопасность