БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ СЕТЕЙ

Цель – приобретение знаний в области обеспечения безопасности информации, передаваемой в корпоративных сетях, контроля трафика в них, овладение методами противодействия кибератакам, а также формирование практических навыков по настройке оборудования для защиты корпоративных сетей

Программа содержит: справочный, теоретический материалы, лабораторные и практические занятия, направленные на решение вопросов обеспечения безопасности корпоративных сетей.

Аудитория

- руководители подразделений информационной безопасности, ответственные за состояние информационной безопасности и организацию работ по созданию систем защиты информации и их заместители;
- аналитики по вопросам компьютерной безопасности, ответственные за анализ состояния информационной безопасности информационных сетей;
- специалисты, ответственные за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам защиты информации;
- главные специалисты всех наименований, обеспечивающие информационную безопасность;
- ведущие специалисты всех наименований, обеспечивающие информационную безопасность;
- системные и сетевые администраторы, ответственные за безопасность информационных сетей организаций, обоснованный выбор и эффективную эксплуатацию средств защиты и средств анализа (контроля) защищенности сетей.

Требуемая предварительная подготовка слушателей:

- владеть знаниями об особенностях функционирования информационных сетей;
- знания по протоколам и службам стека TCP/IP или модели OSI;
- навыки работы в ОС Windows.

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**
	Правовое и организационное обеспечение безопасности корпоративных сетей
1	Методология обеспечения безопасности информации
2	Государственное регулирование деятельности в области обеспечения информационной
3	Противодействие целенаправленным кибератакам
4	Криптографические методы защиты информации
5	Электронная цифровая подпись
6	Безопасность уровня операционных систем
7	Управление рисками информационной безопасности
	Техническое обеспечение безопасности корпоративных сетей
1	Виды spoofing кибератак
2	DoS, DDoS кибератаки
3	Уязвимости DHCP протокола
4	Уязвимости виртуальных локальных сетей
5	Методы аутентификации в протоколах маршрутизации
6	Технологии организации VPN туннелей
7	Протокол AAA
8	Списки управления доступом
9	Программно-аппаратные методы фильтрации трафика
10	Топология сети при использовании межсетевых экранов

11	Обеспечение безопасности клиент-серверного соединения