ТЕХНОЛОГИИ КИБЕРБЕЗОПАСНОСТИ: ОТ SPOOFING-АТАК ДО VPN И МЕЖСЕТЕВЫХ ЭКРАНОВ

Цель программы — сформировать у слушателей знания и практические навыки в области обеспечения кибербезопасности, необходимые для выполнения задач, возлагаемых на лиц, ответственных за обеспечение кибербезопасности, в том числе технической и криптографической защиты информации, обрабатываемой в корпоративных системах.

Выпускники курса получают свидетельство о повышении квалификации в области информационной безопасности государственного образца.

Целевая аудитория:

- руководители структурных подразделений, обеспечивающих кибербезопасность, в том числе техническую и криптографическую защиту информации, распространение и (или) предоставление которой ограничено, и их заместителей;
- специалистов всех наименований и категорий, обеспечивающих кибербезопасность, в том числе техническую и криптографическую защиту информации, распространение и (или) предоставление которой ограничено

Требуемая предварительная подготовка слушателей:

- профессиональные навыки работы на компьютере;
- навыки управления работой информационных систем;
- знания протоколов и служб стека TCP/IP или модели OSI;
- навыки работы в ОС Windows.

Форма обучения – очная (дневная).
Стоимость обучения одного слушателя – 1900 рублей.

Обучение проводится по адресу: г. Минск, ул. К. Цеткин, 24, 11 этаж в соответствии с графиком учебного процесса.

Продолжительность программы – 76 академических часов.

Учебный план курса

№ п/п	Название тем курса
	Законодательство в области обеспечения кибербезопасности
1.	Государственное регулирование деятельности в области обеспечения кибербезопасности
2.	Национальная система обеспечения кибербезопасности
	Методологические основы обеспечения кибербезопасности корпоративных систем.
3.	Управление рисками кибербезопасности
4.	Противодействие целенаправленным кибератакам
5.	Безопасность уровня операционных систем
	Практические аспекты обеспечения кибербезопасности корпоративных систем
6.	Виды spoofing кибератак
7.	DoS, DDoS кибератаки
8.	Уязвимости DHCP и DNS протоколов.
9.	Уязвимости виртуальных локальных сетей.
10.	Методы аутентификации в протоколах маршрутизации.

11.	Технологии организации VPN туннелей.
12.	Контроль доступа пользователей в сеть.
13.	Списки управления доступом.
14.	Программно-аппаратные методы фильтрации трафика.
15.	Топология сети при использовании межсетевых экранов.
16.	Обеспечение безопасности клиент-серверного соединения.
	Особенности криптографической защиты информации
17.	Криптографические методы защиты информации
18.	Электронная цифровая подпись