КИБЕРБЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ СИСТЕМ

Цель программы — сформировать у слушателей знания в области функционирования корпоративных систем, кибербезопасности, в том числе технической и криптографической защиты информации, а также в области основных протоколов и служб стека TCP/IP.

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 заместители;
- специалисты всех наименований и категорий, обеспечивающих кибербезопасность, в том числе техническую и криптографическую защиту информации, распространение и (или) предоставление которой ограничено;

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.

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
	Основы обеспечения кибербезопасности. Законодательство в области обеспечения кибербезопасности.
1.	Кибербезопасность: основные понятия, принципы и проблемы
2.	Государственное регулирование деятельности в области обеспечения кибербезопасности.
3.	Национальная система обеспечения кибербезопасности.
4.	**Правовые и организационные меры по обеспечению кибербезопасности.**
1.	Организационные меры по защите информации. Создание и поддержание инфраструктуры защиты информации в организации
2.	Вопросы повышения надежности информационной инфраструктуры
3.	Разработка и документирование политик информационной безопасности
4.	Управление рисками кибербезопасности. Аудиты в области обеспечения кибербезопасности.
	Технические меры по обеспечению кибербезопасности.
1.	Обеспечение кибербезопасности компьютерных сетей
2.	Вопросы защиты сетевых взаимодействий.
3.	Защита от вредоносных программ
4.	Внутренние нарушители
5.	Безопасность уровня операционных систем (узлов)
6.	Безопасность технологий виртуализации
7.	Средства криптографической защиты информации
8.	Программно-аппаратные методы фильтрации трафика
9.	Автоматизация процессов обеспечения кибербезопасности с использованием систем класса SGRC
	Криптографическая защита информации
1.	Криптографические методы защиты информации
2.	Средства криптографической защиты информации
3.	Технологии электронной цифровой подписи