ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Цель программы — сформировать у слушателей целостное представление об основных принципах и методах обеспечения безопасности информации, а также выработать навыки анализа и оценки уязвимостей информационных систем для обеспечения защиты информации в организации от угроз и атак с целью минимизации ущерба для организации.

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

Целевая аудитория:

- руководители организаций, их заместители;
- руководители структурных подразделений по информационным технологиям и их заместители;
- руководители структурных подразделений, их заместители, специалисты всех наименований и категорий, обеспечивающих информационную поддержку управленческих функций.

Требуемая предварительная подготовка слушателей:

- общие представления об информационных системах, правовых, организационных и технических аспектах функционирования информационных (компьютерных) систем, методах защиты информации, технологии электронной цифровой подписи, системе электронного документооборота;
- навыки работы на компьютере.

Форма обучения – очная (дневная).
Стоимость обучения для одного слушателя – 1050 рублей.

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

Продолжительность программы – 36 академических часов.

Учебный план курса

№ п/п	Название тем курса
	Информация как объект защиты. Нормативное правовое регулирование в области защиты информации и персональных данных в Республике Беларусь
1.	Информация как объект защиты
2.	Законодательные основы по защите информации и персональных данных в Республике Беларусь
	Понятие информации. Основные качества информации с точки зрения информационной безопасности. Информационные системы
3.	Понятие информации. Основные качества информации с точки зрения информационной безопасности
4.	Понятие информационной системы
	Угрозы информационной системы. Анализ рисков
5.	Основные угрозы информационных систем
6.	Анализ рисков информационной безопасности
	Информационные компьютерные сети. Компьютерные атаки. Защита информации в компьютерных сетях
7.	Безопасность веб-приложений.
8.	Информационные компьютерные сети
9.	Удаленные атаки
10.	Особенности защиты информации в компьютерных сетях
	Стандарты и спецификации в области информационной безопасности
11.	Стандарты информационной безопасности
12.	Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC

13.	Европейские критерии безопасности информационных технологий (ITSEC)
14.	Федеральные критерии безопасности информационных технологий США
15.	Единые критерии безопасности информационных технологий
16.	Группа международных стандартов 270000
	Избирательная и полномочная политика безопасности
17.	Политика безопасности
18.	Субъектно-объектные модели разграничения доступа
19.	Аксиомы политики безопасности
20.	Политики и модели доступа
	Аппаратно-программные средства защиты информации
21.	Организация защиты от вирусов
22.	Межсетевые экраны
23.	Средства обнаружения и предотвращения вторжений
24.	Средства предотвращения утечек
	Модель межсетевого взаимодействия OSI. Модель DOD
25.	Описание уровней модели OSI
26.	Описание уровней модели DOD
	Уровни сетевых атак согласно модели OSI
27.	Атаки на физическом уровне
28.	Атаки на канальном уровне
29.	Атаки на сетевом уровне
30.	Атаки на транспортном уровне
31.	Атаки на уровне приложений
	Предмет и задачи криптографии и криптоанализа. Криптографические системы. Алгоритмы шифрования
32.	Предмет и задачи криптографии и криптоанализа
33.	Криптографические системы
34.	Теория сложности и криптография. Алгоритмы шифрования. Односторонние и хеш-функции, их использование в криптографии
35.	Электронно-цифровая подпись
36.	Средства управления криптографическими ключами
37.	Криптографические протоколы