Разработка, внедрение и аудит системы менеджмента информационной безопасности в соответствии с требованиями ISO/IEC 27001:2022 (СТБ ISO/IEC 27001-2016)

Цель программы — сформировать и совершенствовать знания и навыки, необходимые для построения безопасного процесса разработки ПО, ознакомить с лучшими мировыми подходами и практиками.

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

Целевая аудитория:

- менеджеры по информационной безопасности;
- руководители подразделений защиты информации;
- IT – аудиторы и ответственные за разработку и внедрение системы менеджмента информационной безопасности (СМИБ)

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 – 40 академических часов.

Учебный план курса

№ п/п	Название тем курса
	Структуры и стандарты построения систем информационной безопасности на основании процессного подхода
1.	Терминология в области информационной безопасности
2.	Основы процессного подхода в области информационной безопасности
3.	Обзор стандартов и структур построения систем информационной безопасности (ISO/IEC 2700x, COBIT for Information Security, CIS Critical Security Controls for Effective Cyber Defense, NIST Special Publication 800-53. Revision 4 и др.)
4.	Документирование систем менеджмента информационной безопасности (структура и меж-документные зависимости)
	Проведение GAP –анализа на соответствие требованиям ISO/IEC 27001:2022
5.	Сбор первичных сведений об объекте и разработка плана обследования
6.	Проведение обследования на площадке
7.	Анализ собранной информации, разработка и отчетной документации по проекту
8.	Разработка Плана-графика внедрения СМИБ
9.	Определение состава документации СМИБ, необходимой для разработки или модификации
	Выполнение обязательных требований стандарта
10.	Понимание организации и ее контекста
11.	Понимание потребностей и ожиданий заинтересованных сторон
12.	Определение области применения системы менеджмента информационной безопасности
13.	Лидерство и обязательства
14.	Политика
15.	Организационные функции, ответственность и полномочия
16.	Действия в отношении рисков и потенциальных возможностей
17.	Целевые показатели в сфере информационной безопасности и планирование их достижения
18.	Ресурсы
19.	Компетентность
20.	Осведомленность
21.	Коммуникация
22.	Документированная информация
23.	Планирование и управление функционированием
24.	Оценка рисков информационной безопасности
25.	Обработка рисков информационной безопасности
26.	Мониторинг, измерение, анализ и оценка

27.	Внутренний аудит
28.	Анализ системы руководством
29.	Несоответствия и корректирующие действия
30.	Непрерывное улучшение
	Управление риском в СМИБ
31.	Цели и задачи управления рисками
32.	Методика оценки рисков информационной безопасности
33.	Идентификация активов и оценка ценности активов
34.	Идентификация угроз и уязвимостей
35.	Определение уровня риска
36.	Разработка плана обработки рисков и положения о применимости средств управления ИБ (SoA)
	Разработка и внедрение процессов обеспечения информационной безопасности
37.	Политики информационной безопасности
38.	Организация информационной безопасности
39.	Безопасность, связанная с персоналом
40.	Управление активами
41.	Управление доступом
42.	Криптография
43.	Физическая безопасность и защита от окружающей среды
44.	Операционная деятельность по обеспечению безопасности
45.	Безопасность сети
46.	Приобретение, разработка и сопровождение систем
47.	Взаимоотношения с поставщиками
48.	Управление инцидентами в области информационной безопасности
49.	Управление непрерывностью бизнеса
50.	Соответствие
	Сертификация СМИБ
51.	Проведение предварительного аудита перед выходом на сертификацию
52.	Международные и национальные органы по сертификации
53.	Прохождение сертификационного аудита
54.	Разработка Плана устранений несоответствий по результатам сертификации.
	Соответствие законодательным и договорным требованиям
55.	Защита коммерческой тайны
56.	Защита персональных данных
57.	Особенности внедрения СМИБ в банках
58.	Особенности СМИБ в составе системы безопасности критически важных объектов информатизации
59.	Учет требований GDPR