КИБЕРБЕЗОПАСНОСТЬ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Цель программы — углубленное практическое изучение слушателями вопросов сетевой компьютерной безопасности на критически важных объектах информатизации, получение теоретических и практических знаний в области выполнения мероприятий по проектированию, созданию и аудиту системы информационной безопасности критически важных объектов информатизации.

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

Целевая аудитория:

- руководители подразделения технической защиты информации (работники такого подразделения (уполномоченные должностные лица)), ответственные за выполнение работ по технической и криптографической защите информации, обрабатываемой на КВОИ;
- главные специалисты всех наименований, обеспечивающие техническую и криптографическую защиту информации на КВОИ;
- ведущие специалисты всех наименований, обеспечивающие техническую и криптографическую защиту информации на КВОИ;
- специалисты всех наименований и категорий, обеспечивающие техническую и криптографическую защиту информации на КВОИ;
- специалисты, ответственные за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам технической и криптографической защиты информации, обрабатываемой на КВОИ.

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 – 1050 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
	Правовые аспекты в сфере защиты информации в Республике Беларусь.
1.	Актуальность проблемы обеспечения защиты информации.
2.	Базовые термины и определения.
3.	Правовое регулирование безопасности КВОИ в Республике Беларусь.
4.	Стандарты и рекомендации.
5.	Ответственность за нарушения законодательства
	Обеспечение информационной безопасности критически важных объектов информатизации
6.	Концепция информационной безопасности (в отношении КВОИ).
7.	Требования по обеспечению информационной безопасности КВОИ.
8.	Особенности и порядок отнесения объектов информатизации к КВОИ.
9.	Обязанности владельцев КВОИ.
10.	Проектирование и создание системы информационной безопасности КВОИ.
11.	Организационная структура системы информационной безопасности КВОИ.

12.	Аудит системы информационной безопасности КВОИ.
	Защита КВОИ в соответствии с приказом ОАЦ от 20.02.2020 №66 и СТБ ISO/IEC 27001-2016.
13.	Стандарты серии СТБ ISO/IEC 2700x.
14.	Подход на основе анализа и управления рисками.
15.	Практическое руководство по внедрению СМИБ.
16.	Определение физических и логических границ.
17.	Инвентаризация и составление реестра активов.
18.	Классификация активов и категорирование информации.
19.	Выявление возможных угроз, построение модели угроз.
20.	Определение вероятности реализации угроз.
21.	Разработка полного пакета документации (концепции, политики, регламенты, инструкции, паспорта и пр.).
22.	Разработка методологии оценки рисков.
23.	Анализ рисков, количественные и качественные значения рисков.
24.	Формирование плана обработки риска.
25.	Первоочередные мероприятия по повышению безопасности.
26.	Акт применимости средств управления защитой информации.
27.	Контроль защитных мер и аудит информационной безопасности.
28.	Повышение осведомленности персонала.
	Международные стандарты и лучшие мировые практики по защите критической инфраструктуры NIST, CIS, SANS 20.
29.	Идентификация оборудования и программного обеспечения.
30.	Безопасная конфигурация программного и аппаратного обеспечения.
31.	Ограничение и контроль сетевых протоколов, портов и служб.
32.	Контроль и защита беспроводных устройств.
33.	Защита от вредоносного кода.
34.	Непрерывный анализ и устранение уязвимостей.
35.	Управление журналами регистрации событий.
36.	Обработка инцидентов информационной безопасности.
37.	Проведение обучения, тренировок и тестирования.
	Автоматизация процессов обеспечения информационной безопасности критически важных объектов информатизации с использованием систем класса SGRC.
38.	Автоматизация процесса проведения инвентаризации и составления реестра активов.
39.	Автоматизация процесса проведения аудитов объектов КВОИ.
40.	Автоматизация процесса оценки рисков объектов КВОИ.