ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Цель – углубленное практическое изучение слушателями вопросов сетевой компьютерной безопасности на критически важных объектах информатизации.

Аудитория

- руководители подразделения технической защиты информации (работники такого подразделения (уполномоченные должностные лица)), ответственные за выполнение работ по технической и криптографической защите информации, обрабатываемой на критически важных объектах информатизации;
- 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)

Обучение проводится отделом образовательных услуг республиканского унитарного предприятия «Национальный центр обмена трафиком» по адресу: г. Минск, ул. К.Цеткин, 24, в соответствии с графиком учебного процесса

Программа рассчитана на 36 часов учебных занятий.

Учебно-тематический план

№ п/п	**Название тем**
	Правовые аспекты в сфере защиты информации в Республике Беларусь.
1.1	Актуальность проблемы обеспечения защиты информации
1.2	Базовые термины и определения
1.3	Правовое регулирование безопасности КВОИ в Республике Беларусь
1.4	Стандарты и рекомендации
1.5	Ответственность за нарушения законодательства
	Обеспечение информационной безопасности критически важных объектов информатизации
2.1	Концепция информационной безопасности (в отношении КВОИ)
2.2	Требования по обеспечению информационной безопасности критически важных объектов информатизации (КВОИ)
2.3	Особенности и порядок отнесения объектов информатизации к КВОИ
2.4	Обязанности владельцев КВОИ
2.5	Проектирование и создание системы информационной безопасности КВОИ
2.6	Организационная структура системы информационной безопасности КВОИ
2.7	Аудит системы информационной безопасности КВОИ
	Защита КВОИ в соответствии с приказом ОАЦ от 20.02.2020 №66 и СТБ ISO/IEC 27001-2016
3.1	Стандарты серии СТБ ISO/IEC 2700х
3.2	Подход на основе анализа и управления рисками
3.3	Практическое руководство по внедрению СМИБ
3.4	Определение физических и логических границ
3.5	Инвентаризация и составление реестра активов
3.6	Классификация активов и категорирование информации

3.7	Выявление возможных угроз, построение модели угроз
3.8	Определение вероятности реализации угроз
3.9	Разработка полного пакета документации (концепции, политики, регламенты, инструкции, паспорта и
3.10	Разработка методологии оценки рисков
3.11	Анализ рисков, количественные и качественные значения рисков
3.12	Формирование плана обработки риска
3.13	Первоочередные мероприятия по повышению безопасности
3.14	Акт применимости средств управления защитой информации
3.15	Контроль защитных мер и аудит информационной безопасности
3.16	Повышение осведомленности персонала
	Международные стандарты и лучшие мировые практики по защите критической инфраструктуры NIST, CIS, SANS 20
4.1	Идентификация оборудования и программного обеспечения
4.2	Безопасная конфигурация программного и аппаратного обеспечения
4.3	Ограничение и контроль сетевых протоколов, портов и служб
4.4	Контроль и защита беспроводных устройств
4.5	Защита от вредоносного кода
4.6	Непрерывный анализ и устранение уязвимостей
4.7	Управление журналами регистрации событий
4.8	Обработка инцидентов информационной безопасности
4.9	Проведение обучения, тренировок и тестирования