Основные практики обеспечения информационной безопасности + КИБЕРУЧЕНИЯ

Цель программы — углубленное практическое изучение слушателями вопросов сетевой компьютерной безопасности.

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

Целевая аудитория:

- специалисты центров мониторинга инцидентов информационной безопасности;
- лицензиаты Оперативно-аналитического центра при Президенте Республики Беларусь и соискатели лицензии на деятельность по технической защите информации;
- технические специалисты подразделений, реализующих мероприятия по технической и/или криптографической защите информации в организациях, в том числе на критически важных объектах информатизации.

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 – 3500 рублей.

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

Продолжительность программы – 56 академических часов.

Учебный план курса

№ п/п	Название тем курса
	Основы информационной безопасности.
1.	Цели и задачи мероприятия. Обзор программы. Основы и задачи информационной безопасности. Управление ИБ. Система менеджмента ИБ. Направления развития ИБ в международной практике.
2.	Практические аспекты внедрения системы управления ИБ на предприятии. Риск-ориентированный подход.
3.	Практика: описание бизнес-процессов, определение области деятельности системы управления ИБ Этапы процесса управления рисками ИБ. Практика: оценка ценности активов.
	Управление рисками и инцидентами ИБ.
4.	Оценка рисков ИБ. Обработка рисков ИБ. Лекция: основы работы с инцидентами ИБ.
5.	Лекция: управление событиями и инцидентами ИБ. Практика: Знакомство с SIEM Просмотр и фильтрация событий. Сценарий на киберполигоне: один день из жизни оператора SOC Анализ результатов, обсуждение и разбор сценария.
	Безопасность ОС.
6.	Лекция: Архитектура безопасности ОС Linux Практика: настройка прав доступа к общим ресурсам для удаленных пользователей Лекция: мониторинг и обнаружение атак в ОС Linux.
7.	Практика: поиск следов атак на скомпрометированных хостах, анализ журналов событий ОС Linux. Лекция: мониторинг и обнаружение атак в ОС Windows. Практика: поиск следов атак на скомпрометированных хостах, анализ журналов событий.

	Сетевая безопасность.
8.	Лекция: архитектура защищенной сети. Лекция: Анализ сетевого трафика. Практика: анализ неизвестного трафика в wireshark.
9.	Практика: настройка блокирования нежелательного трафика в iptables. Лекция: системы обнаружения вторжений. Практика: настройка обнаружения подозрительного трафика в suricata.
	Киберучения.
10.	Сценарий на киберполигоне: атака вируса-шифровальщика. Анализ результатов, обсуждение и разбор сценария.
11.	Настройка защитных мер в инфраструктуре. Сценарий на киберполигоне: атака скриптами. Проверка реализованной системы защиты. Анализ результатов, работа над ошибками. Разбор атак.