ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ

Цель программы — углубленное практическое изучение слушателями вопросов кибербезопасности, формирование у слушателей целостного представления о функционировании национальной системы обеспечения кибербезопасности.

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

Целевая аудитория:

- руководители центров кибербезопасности;
- руководители структурных подразделений;
- специалисты центров кибербезопасности;
- специалисты всех наименований и категорий, обеспечивающие кибербезопасность в организациях.

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 – 1900 рублей.

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

Продолжительность программы – 76 академических часов.

Учебный план курса

№ п/п	Название тем курса
	Нормативное правовое регулирование вопросов кибербезопасности в Республике Беларусь.
1.	Кибербезопасность, информационная безопасность, защита информации. Международный опыт противодействия киберберпреступности. Методология построения национальной системы обеспечения кибербезопасности.
2.	Государственное регулирование деятельности в сфере обеспечения кибербезопасности
3.	Требования по кибербезопасности объектов информационной инфраструктуры государственных органов и иных организаций.
	Системы управления информационной безопасностью и событиями безопасности (SIEM).
4.	SIEM-системы. Краткий обзор существующих решений. Сертифицированные open-source и коммерческие решения в Республике Беларусь.
5.	Архитектура SIEM. Установка и настройка основных компонентов.
6.	Типы источников событий информационной безопасности. Теоретические аспекты подключения источников событий ИБ в SIEM (события Windows/Linux, СУБД, телекоммуникационного оборудования, антивируса, NGFW с функцией ips)
7.	Подключение основных источников событий ИБ в SIEM.
8.	Нормализация (приведение событий ИБ от различных источников к единому виду), написание правил нормализации событий ИБ.
9.	Написание правил корреляции и агрегации событий ИБ для различных типов источников (конструкторы правил корреляции, язык написания правил корреляции и основные операнды)
10.	Создание графиков, отчетов, формирование дашбордов
11.	Настройка отправки сработок правил корреляции (smtp, tcp/udp). Реагирование подразделения мониторинга на инцидент ИБ
12.	Порядок регистрации КИ. Порядок взаимодействия центра кибербезопасности с национальным центром кибербезопасности

	Система управления информационной безопасностью и событиями безопасности (SIEM) на примере решения, используемого организацией, от конкретного вендора (Max Patrol, KUMA, SOAR, ArcSight, Wazuh и пр.).
	Модуль 1 - Max Patrol SIEM.
13.	Назначение MaxPatrol SIEM. Asset management, vulnerability management, SIEM. Компоненты системы, направления развития, потоки данных.
14.	Установка системы MaxPatrol SIEM. Установка системы обновлений UCS. Работа с PT KB.
15.	Журналы и устранение неполадок.
16.	Пользователи и роли.
17.	Сбор и работа с событиями. PDQL и таксономия событий.
18.	Нормализация, обогащение и корреляция событий. Работа с PT KB.
19.	Загрузка событий из файла и отладка. Агрегация инцидентов.
20.	Доставка уведомлений. Создание виджетов.
	Оценка защищенности инфраструктуры. Реагирование на киберинциденты.
21.	Реагирование на киберинциденты. Подготовительные, организационные и практические мероприятия.
22.	Основные принципы и инструменты выявления, анализа действий нарушителя и работы вредоносного программного обеспечения.