Администрирование Континент 4

Цель программы — получение теоретических знаний и практических навыков, необходимых для внедрения, настройки и обслуживания сетевых компонентов Континент 4.

Выпускники курса получают свидетельство о повышении квалификации государственного образца.

Целевая аудитория:

- системные администраторы;
- руководители IT-служб;
- архитекторы систем информационной безопасности;
- специалисты в сфере информационной безопасности, которые отвечают за защиту сегментов корпоративной сети организации и ее филиалов, разделенных каналами связи общего доступа.

Форма обучения – очная (дневная).

Стоимость обучения одного слушателя – 4500 рублей.

Обучение проводится по адресу: г. Минск, ул. К. Цеткин, 24, (1 или 11 этаж) в соответствии с графиком учебного процесса.

Продолжительность программы – 40 академических часов (5 дней).

Учебный план курса

№ п/п	Название тем курса
I.	**Общие сведения по Континент 4**
1.	Назначение и состав комплекса.
2.	Принципы функционирования комплекса.
3.	Управление комплексом.
4.	ПАК "Соболь".
5.	Типовые аппаратные платформы и их производительность.
6.	Политика лицензирования.
7.	Порядок ввода комплекса в эксплуатацию.
8.	**Лабораторный модуль №1 "Развертывание ЦУС Континент, рабочего места главного администратора и подчиненных узлов безопасности"**
9.	Лабораторная работа №1 "Развертывание центра управления сетью Континент и регистрация главного администратора".
10.	Лабораторная работа №2 "Подготовка рабочего места главного администратора".
11.	Лабораторная работа №3 "Настройка подключения к подсистеме мониторинга".
12.	Лабораторная работа №4 "Развертывание подчиненных узлов безопасности".
II.	**Управление узлами Континент.**
13.	Роли администраторов. Назначение администраторов.
14.	Дистанционный доступ по протоколу SSH.
15.	**Лабораторный модуль №2 "Управление узлами Континент".**
16.	Лабораторная работа №1 "Управление ролями и учетными записями администраторов".
17.	Лабораторная работа №2 "Настройка дистанционного доступа по протоколу SSH".
III.	**Настройка межсетевого экранирования.**
18.	Обработка трафика узлом безопасности.
19.	Межсетевое экранирование.
20.	Сетевые функции.

21.	Виды объектов ЦУС.
22.	Правила фильтрации.
23.	Правила трансляции.
24.	Установка политики.
25.	**Лабораторный модуль №3 "Настройка многофункционального межсетевого экрана на узлах безопасности в режиме UTM".**
26.	Лабораторная работа №1 "Настройка правил фильтрации".
27.	Лабораторная работа №2 "Настройка правил трансляции".
IV.	**Система обнаружения и предотвращения вторжений.**
28.	Концепция управления СОВ.
29.	Управление детектором атак в режимах Monitor и Inline.
30.	Установка БРП. Создание собственных сигнатур.
31.	Формирование и установка политик СОВ.
32.	**Лабораторный модуль №4 "Инициализация, настройка и проверка функциональности детектора атак".**
33.	Лабораторная работа №1 "Инициализация детектора атак".
34.	Лабораторная работа №2 "Настройка детектора атак: установка БРП, создание профиля и применение политик".
35.	Лабораторная работа №3 "Проверка функциональности детектора атак".
36.	Лабораторная работа №4 "Настройка СОВ в составе UTM-узла безопасности".
V.	**Построение VPN.**
37.	VPN-туннель.
38.	Шифрование.
39.	Топология.
40.	L3VPN IPsec.
41.	VPN удаленного доступа.
42.	L2VPN-туннель.
43.	**Лабораторный модуль №5 "Построение VPN".**
44.	Лабораторная работа №1 "Организация проприетарного L3VPN между защищаемыми сетями".
45.	Лабораторная работа №2 "Построение L3VPN IPSec между пересекающимися сетями".
46.	Лабораторная работа №3 "Организация L3VPN между удаленным пользователем и защищаемой сетью".
47.	Лабораторная работа №4 "Организация L3VPN между удаленным пользователем и защищаемой сетью за другим УБ Континент".
48.	Лабораторная работа №5 "Организация L2VPN".
VI.	**Обеспечение отказоустойчивости комплекса.**
49.	Резервирование и восстановление конфигурации.
50.	Аппаратное резервирование и восстановление узла безопасности.
51.	Резервирование БД ЦУС.
52.	**Лабораторный модуль №6 "Резервирование и восстановление".**
53.	Лабораторная работа №1 "Резервирование узла безопасности".
54.	Лабораторная работа №2 "Резервирование БД ЦУС".
55.	Лабораторная работа №3 "Резервное копирование и восстановление данных узла безопасности или ЦУС".
VII.	**Мониторинг и аудит.**
56.	Общие сведения по системе мониторинга: инициализация, объекты мониторинга и типы информации, применение правил и шаблонов.
57.	Просмотр сведений журналов.
58.	Аудит.
59.	**Лабораторный модуль №7 "Мониторинг и аудит".**

60.	Лабораторная работа №1 "Настройка параметров аудита. Работа с подсистемой мониторинга".
61.	Лабораторная работа №2 "Локальная работа с журналами аудита".
VIII.	**Настройка Multi-WAN.**
62.	**Лабораторный модуль №8 "Настройка Multi-WAN".**
63.	Лабораторная работа №1 "Обеспечение отказоустойчивости канала связи".
64.	Лабораторная работа №2 "Настройка балансировки трафика между двумя внешними интерфейсами узла безопасности".
IX.	**Виртуальная маршрутизация.**
65.	Краткое описание механизма виртуальной маршрутизации.
66.	Настройка VRF-зон.
67.	Просмотр сведений о VRF-зонах в локальном меню узла безопасности.
68.	Управление сетевыми интерфейсами в составе VRF-зоны.
69.	**Лабораторный модуль №9 "Настройка и применение виртуальной маршрутизации".**
70.	Лабораторная работа №1 "Настройка и применение виртуальной маршрутизации".
X.	**Поддержка динамической маршрутизации.**
71.	Протоколы динамической маршрутизации.
72.	**Лабораторный модуль №10 "Поддержка динамической маршрутизации".**
73.	Лабораторная работа №1 "Настройка динамической маршрутизации по протоколу BGP"