Бауманский учебный центр «Специалист»

Программа курса Сертифицированный администратор Check Point R82

Код курса: **ЧЕКПОЙТ3**

Тема	Ак. часов
Модуль 1. Введение в управление механизмами безопасности средствами Check Point Quantum • Обзор механизмов управления, трехзвенная архитектура. • SmartConsole, типы интерфейсов, режимы работы. • Сервер управления. • Шлюз безопасности. • Операционная система Gaia, виды оболочек. • Web-портал Gaia. **Лабораторная работа.** Знакомство с операционной системой Gaia. **Лабораторная работа.** Подключение SmartConsole к серверу управления, работа в SmartConsole.	**2**
Модуль 2. Управление учетными записями администраторов • Основы работы с учетными записями администраторов. • Администраторы SmartConsole. • Понятие сессии администрирования, особенности и возможности. • Последовательность операций в рамках сессии администрирования. • Советы и рекомендации. **Лабораторная работа.** Управление учетными записями администраторов и их доступом.	**2**
Модуль 3. Управление объектами • Обзор объектов, доступных в SmartConsole. • Советы и рекомендации. **Лабораторная работа.** Просмотр и редактирование объектов.	**2**
Модуль 4. Управление политиками безопасности • Введение в политику безопасности. • Настройка политики управления доступом (Access Control Policy). • Обзор механизмов трансляции адресов. • Настройка политики трансляции адресов. **Лабораторная работа.** Управление политиками безопасности.	**3**
Модуль 5. Работа со слоями • Концепция слоя, слои политики управления доступом. • Упорядоченные и вложенные слои. • Порядок обработки правил при наличии слоев. • Советы и рекомендации. **Лабораторная работа.** Упорядоченные слои. **Лабораторная работа.** Вложенные слои.	**3**

Модуль 6. Мониторинг обеспечения безопасности • Обзор механизмов мониторинга. • Просмотр лог-записей в SmartConsole. • Утилита SmartView Monitor. • Просмотр логов через Web-приложение SmartView. • Советы и рекомендации. **Лабораторная работа.** Мониторинг трафика. **Лабораторная работа.** Мониторинг состояния системы.	**3**
Модуль 7. Аутентификация пользователей с помощью механизма Identity Awareness • Обзор технологии Identity Awareness. • Принципы работы. • Последовательность действий при работе Identity Awareness. • Советы и рекомендации. **Лабораторная работа.** Применение Identity Awareness.	**2**
Модуль 8. Расшифровка HTTPS • Обзор технологии расшифровки. • Механизмы и принципы работы расшифровки. • Последовательность действий при расшифровке. • Советы и рекомендации. **Лабораторная работа.** Улучшение защиты с помощью расшифровки HTTPS.	**3**
Модуль 9. Управление приложениями и фильтрация URL • Основы и принципы действия управления приложениями и фильтрации URL. • Последовательность действий. • Советы и рекомендации. **Лабораторная работа.** Формирование унифицированной политики безопасности.	**2**
Модуль 10. Введение в механизмы защиты от атак (Treat Prevention) • Что такое режим Autonomous Threat Prevention? • Основы функционирования режима Autonomous Threat Prevention. • Последовательность действий при работе режима Autonomous Threat Prevention.	**2**
Аудиторная нагрузка в классе с преподавателем	**24 ак.ч. + 24 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru