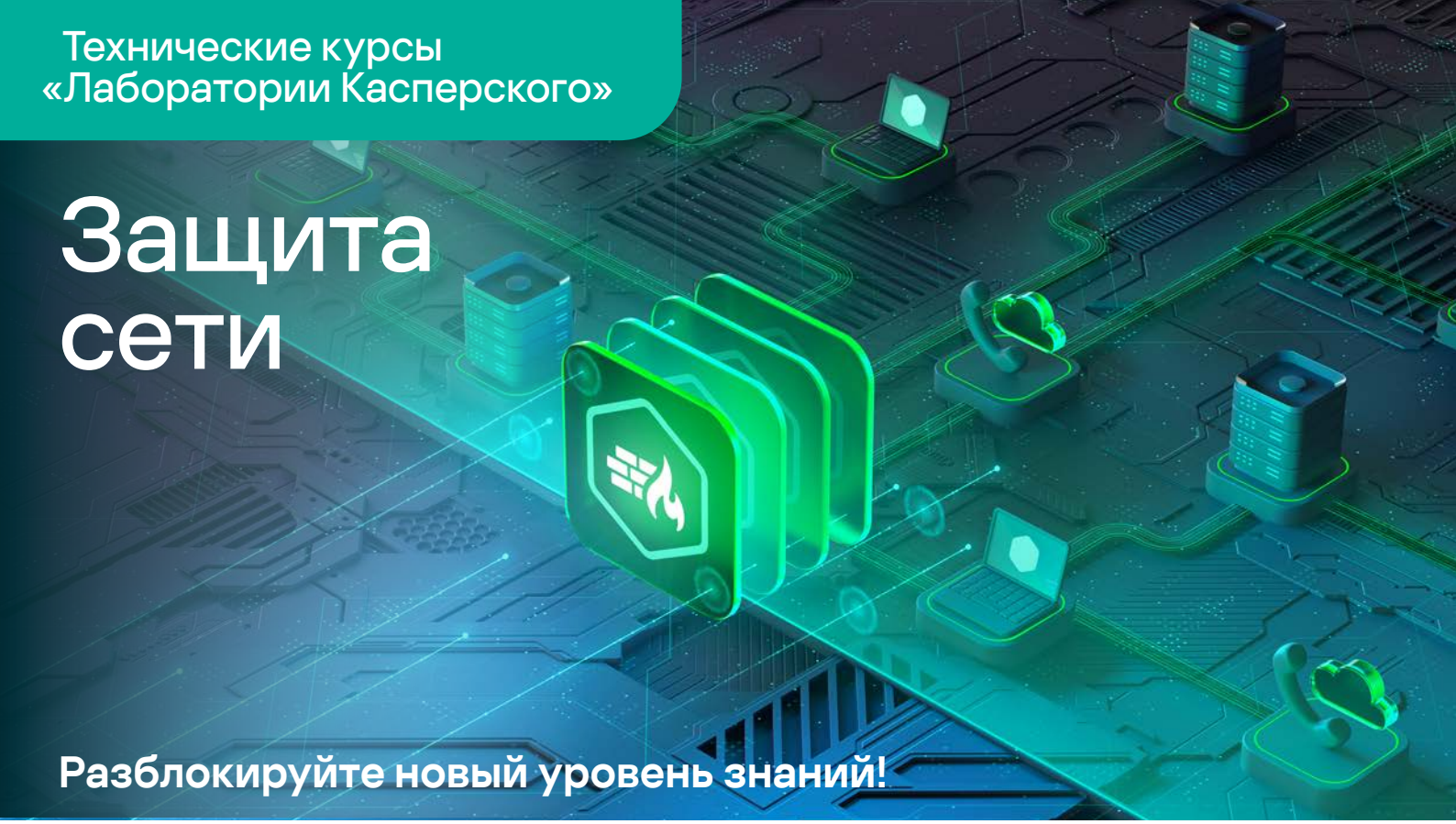
Технические курсы
«Лаборатории Касперского»

Защита сети



Разблокируйте новый уровень знаний!

Погрузитесь в новые знания с **Авторизованными Учебными Центрами «Лаборатории Касперского».** Тренинги по продукту для бизнеса от лидера решений в сфере IT-безопасности повысят ваш профессиональный уровень и расширят перспективы.

KL 004. Kaspersky SD-WAN

Kaspersky SD-WAN является решением корпоративного класса для централизованного программного управления WAN сегментом сети. Курс знакомит с архитектурой и возможностями решения, рассказывает и показывает, как выполнить настройку решения на многочисленных примерах.

Материалы курса включают слайды с описанием принципов работы, настройки и поиска неисправностей, а также лабораторные работы для закрепления практических навыков настройки.

По окончании курса слушатели смогут:

- Понимать, какие недостатки традиционных сетей могут быть преодолены внедрением программно-определяемых глобальных сетей;
- Различать типы транспортных сервисов, понимать особенности их работы;
- Создавать новые транспортные сервисы, управлять существующими;
- Настраивать правила выбора канала в зависимости от текущего состояния всех доступных каналов;
- Управлять динамической маршрутизацией внутри сети SD-WAN, а также на стыке с legacy сетью.

kaspersky

KL 007. Kaspersky NGFW

Kaspersky NGFW — это комплексное решение корпоративного класса для эффективной защиты корпоративных сетей от современных киберугроз. Курс посвящен освоению функционала, особенностей архитектуры и методик настройки данного решения.

Программа курса охватывает широкий спектр вопросов: начиная от базовой настройки устройства и заканчивая управлением различными модулями безопасности и работой с внешними системами.

Основные цели курса: изучение архитектурных особенностей и функций Kaspersky NGFW, освоение методов настройки и диагностики устройства, практическое овладение средствами сегментирования, изоляции и фильтрации трафика, овладение методами настройки и контроля NAT, глубоких проверок пакетов (DPI), SSL Inspection, DNS Security, Web Control, антивирусной защиты и IDS/IPS.

В результате успешного освоения курса слушатели научатся:

- Понимать, какие современные угрозы и вызовы могут быть нейтрализованы внедрением межсетевого экрана нового поколения;
- Разбираться в архитектуре и схеме обработки трафика NGFW, понимать взаимодействие модулей безопасности;
- Выполнять базовую настройку NGFW, управлять сетевыми объектами и правилами фильтрации;
- Настраивать и управлять ключевыми модулями безопасности: App-Control, IDPS, антивирус, веб-контроль и фильтрация DNS;
- Настраивать и применять политики расшифровки и инспектирования TLS/ SSL трафика для противодействия скрытым угрозам;
- Реализовывать трансляцию сетевых адресов (NAT) и настраивать динамическую маршрутизацию (BGP);
- Организовывать интеграцию NGFW с внешними системами (KNBE, платформа OSMP, Zabbix) для автоматизации и мониторинга.