



# Программы тренингов «Лаборатории Касперского»

---

**для специалистов  
по IT-безопасности**

**kaspersky**

Подробнее на [kaspersky.ru](https://kaspersky.ru)  
#активируйбудущее

# Тренинги для специалистов по IT-безопасности

Количество и сложность угроз постоянно растет, и для успешной защиты от них требуются не только передовые решения, но и квалифицированные сотрудники. Тренинги «Лаборатории Касперского» помогут IT-профессионалам получить актуальные знания, расширить свою экспертизу и развить практические навыки в выбранных областях кибербезопасности.

Тренинги охватывают широкий спектр тем в области кибербезопасности, а также различные методики и практик, которые могут быть полезны как начинающим специалистам, так и опытным экспертам.

Все тренинги сочетают теоретическую и практическую часть. По завершении курса проводится оценка усвоенного участниками материала.

Тренинги проводятся на территории заказчика или в региональных офисах «Лаборатории Касперского».

## Преимущества тренингов

### Цифровая криминалистика и продвинутая цифровая криминалистика

Повысьте экспертизу ваших экспертов в области цифровой криминалистики и реагирования на инциденты. Задача тренингов – укрепить знания специалистов во всем, что касается поиска следов киберпреступления и анализа различных типов данных с целью установить источник и временные параметры атаки. После завершения тренинга участники смогут успешно проводить расследование компьютерных инцидентов, что повысит уровень безопасности компании в целом.

### Анализ вредоносного ПО и обратная разработка (начальный и экспертный уровни)

Тренинг по обратной разработке поможет специалистам в области реагирования на инциденты успешнее проводить расследование вредоносных атак. Курс предназначен для сотрудников IT-департамента и системных администраторов. В ходе тренинга участники учатся анализировать вредоносное ПО, собирать индикаторы компрометации (IoCs), писать сигнатуры для обнаружения вредоносного ПО или зараженных машин, а также восстанавливать зараженные/зашифрованные файлы и документы.

### Реагирование на инциденты

Тренинг поможет сотрудникам службы IT-безопасности больше узнать обо всех стадиях расследования инцидентов и даст все необходимые сведения для успешного самостоятельного устранения последствий инцидента.

### YARA

Тренинг поможет узнать, как правильно писать, эффективно тестировать и улучшать правила YARA таким образом, чтобы с помощью них можно было успешно обнаруживать атаки.

### Администрирование Kaspersky Anti Targeted Attack Platform

Тренинг по администрированию Kaspersky Anti Targeted Attack Platform (KATA) позволит узнать, как установить и настроить решение, а также как управлять им с максимальной эффективностью.

### Анализ инцидентов Kaspersky Anti Targeted Attack Platform

Тренинг включает в себя множество упражнений, основанных на часто встречающихся на практике сценариях обнаружения угроз. Важную роль в них играет обработка уведомлений KATA – отслеживание, интерпретация, реагирование.

## Успешный практический опыт

«Лаборатория Касперского» обладает обширным опытом обнаружения и исследования угроз. Эксперты компании – специалисты с мировым именем – обладают самой свежей, детальной и уникальной информацией о способах борьбы с кибератаками.

Темы	Продолжительность	Навыки
<b>Цифровая криминалистика</b>		
<ul style="list-style-type: none"><li>Введение в цифровую криминалистику</li><li>Оперативное реагирование и сбор цифровых улик</li><li>Внутренняя структура реестра Windows</li><li>Анализ артефактов в Windows</li><li>Криминалистический анализ браузера</li><li>Анализ электронной почты</li></ul>	5 дней	<ul style="list-style-type: none"><li>Организация лаборатории цифровой криминалистики</li><li>Сбор цифровых улик и порядок обращения с ними</li><li>Воссоздание хронологической картины инцидента с помощью временных меток</li><li>Выявление следов вторжения посредством анализа артефактов в ОС Windows</li><li>Анализ истории браузера и электронной почты</li><li>Эффективное применение средств и методов цифровой аналитики</li></ul>
<b>Анализ и обратная разработка вредоносного ПО</b>		
<ul style="list-style-type: none"><li>Цели и методы анализа и обратной разработки вредоносного ПО</li><li>Внутреннее устройство ОС Windows, исполняемые файлы, ассемблер x86</li><li>Базовые методы статического анализа (извлечение строк, анализ импортов, анализ точек входа исполняемого файла, автоматическая распаковка и т. д.)</li><li>Базовые методы динамического анализа (отладка, инструменты мониторинга, перехват трафика и т. д.)</li><li>Анализ файлов .NET, Visual Basic, Win64</li><li>Методы анализа скриптов и программ, отличных от исполняемых файлов (пакетные файлы, AutoIt, Python, JScript, JavaScript, VBS)</li></ul>	5 дней	<ul style="list-style-type: none"><li>Построение безопасной среды для анализа вредоносных программ: развертывание «песочницы» и всех необходимых инструментов</li><li>Понимание принципов исполнения программ в ОС Windows</li><li>Распаковка, отладка и анализ вредоносного объекта, определение его функций</li><li>Обнаружение вредоносных сайтов путем анализа вредоносных скриптов</li><li>Проведение экспресс-анализа вредоносных программ</li></ul>
<b>Цифровая криминалистика (экспертный уровень)</b>		
<ul style="list-style-type: none"><li>Экспертная криминалистика в ОС Windows</li><li>Восстановление данных</li><li>Сетевая и облачная криминалистика</li><li>Криминалистический анализ дампов памяти</li><li>Хронологический анализ</li><li>Практическая криминалистика реальных целевых атак</li></ul>	5 дней	<ul style="list-style-type: none"><li>Глубокий анализ файловой системы</li><li>Восстановление удаленных файлов</li><li>Анализ сетевого трафика</li><li>Обнаружение вредоносной активности по дампам памяти</li><li>Восстановление хронологии инцидента</li></ul>
<b>Анализ и обратная разработка вредоносного ПО (экспертный уровень)</b>		
<ul style="list-style-type: none"><li>Методы расширенного статического и динамического анализа (статический анализ шелл-кода, синтаксический анализ заголовка исполняемого файла, блоки переменных окружения потока (TEB) и окружения процесса (PEB), загрузка функций на основе различных алгоритмов хэширования)</li><li>Методы расширенного динамического анализа (структура исполняемого файла, ручная и экспертная распаковка, распаковка вредоносных архивов, содержащих полный исполняемый файл в зашифрованной форме)</li><li>Обратная разработка APT-угроз (полная проработка сценария APT-атаки, начиная с фишингового сообщения электронной почты и заканчивая как можно более глубоким анализом)</li><li>Анализ протоколов (анализ зашифрованных коммуникаций по протоколу C2, методы расшифровки трафика)</li><li>Анализ руткитов и буткитов (отладка загрузочного сектора при помощи IDA и VMWare, отладка ядра при помощи двух виртуальных машин, анализ образцов руткитов)</li></ul>	5 дней	<ul style="list-style-type: none"><li>Использование передовых методов обратной разработки и распознавание методов защиты от обратной разработки (обфускация, защита от отладки)</li><li>Расширенный анализ руткитов и буткитов</li><li>Анализ шелл-кода эксплойтов, внедренного в различные виды файлов, а также вредоносных программ для сред, отличных от Windows</li></ul>

Темы	Продолжительность	Навыки
<b>Реагирование на инциденты</b>		
<ul style="list-style-type: none"> <li>Общие сведения о реагировании на инциденты</li> <li>Обнаружение и первичный анализ</li> <li>Цифровой анализ</li> <li>Создание правил обнаружения (YARA, Snort, Bro)</li> </ul>	5 дней	<ul style="list-style-type: none"> <li>Отличие АРТ от других типов угроз</li> <li>Понимание различных методов атаки и анатомии целевых атак</li> <li>Применение специальных методов мониторинга и обнаружения</li> <li>Выполнение процедуры реагирования на инциденты</li> <li>Восстановление хронологической картины и логики инцидента</li> <li>Создание правил обнаружения и подготовка отчетов</li> </ul>
<b>YARA</b>		
<ul style="list-style-type: none"> <li>Введение в синтаксис правил YARA</li> <li>Способы быстрого и эффективного создания правил YARA-генераторы</li> <li>Тестирование правил YARA на ложные срабатывания</li> <li>Поиск новых необнаруженных образцов с помощью VirusTotal</li> <li>Использование внешних модулей в YARA для эффективного поиска угроз</li> <li>Поиск аномалий</li> <li>Множество примеров из реальной практики</li> <li>Набор упражнений для совершенствования навыков работы с YARA</li> </ul>	2 дня	<ul style="list-style-type: none"> <li>Создание эффективных правил YARA</li> <li>Тестирование правил YARA</li> <li>Дальнейшее совершенствование правил для эффективного обнаружения угроз</li> </ul>
<b>Администрирование KATA</b>		
<ul style="list-style-type: none"> <li>Стандартная схема развертывания решения и размещения серверов</li> <li>Системные требования</li> <li>Модель лицензирования</li> <li>Сервер «песочницы»</li> <li>Консоль Central Node</li> <li>Сенсоры</li> <li>Интеграция с инфраструктурой</li> <li>Установка сенсора на рабочих станциях</li> <li>Добавление лицензии и обновление баз</li> <li>Алгоритм работы решения</li> </ul>	1 день	<ul style="list-style-type: none"> <li>Создание плана развертывания, оптимального для среды заказчика</li> <li>Установка и настройка компонентов KATA</li> <li>Поддержка и управление решением</li> </ul>
<b>Анализ инцидентов KATA</b>		
<ul style="list-style-type: none"> <li>Интерпретация уведомлений (алертов) KATA</li> <li>Объяснение технологий обнаружения и анализа</li> <li>Объяснение механизмов скоринга и оценки риска</li> </ul>	1 день	<ul style="list-style-type: none"> <li>Понимание того, как работает скоринг и как он используется механизмами оценки риска</li> <li>Способность уверенно работать с уведомлениями KATA: отслеживать, интерпретировать, реагировать</li> </ul>

[www.kaspersky.ru](http://www.kaspersky.ru)

© 2023 АО «Лаборатория Касперского». Все права защищены. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.