



# Kaspersky xTraining

Раскройте потенциал вашей  
ИБ-команды с помощью  
мировой экспертизы  
«Лаборатории Касперского»

**kaspersky** активируй  
будущее

[kaspersky.ru](https://kaspersky.ru)

### ● Самостоятельное онлайн-обучение

Учитесь в удобное время и комфортном темпе из любой точки мира

### ● Много практики

Отрабатывайте навыки обеспечения кибербезопасности в безопасной виртуальной среде, изучая реальные случаи кибератак

### ● Лучшие преподаватели

Получите уникальные советы, стратегии и знания от ведущих мировых экспертов-практиков в области ИБ

### ● Поддержка и обратная связь

Используйте портал поддержки для получения ответов на интересующие вас вопросы

### ● Сертификат о прохождении

Получите PDF-сертификат на бланке «Лаборатории Касперского» с подписью эксперта(-ов) курса, чтобы повысить ваш престиж в глазах работодателя

# Время вывести вашу ИБ-команду на новый уровень

Kaspersky xTraining – это ответ на постоянно меняющийся ландшафт киберугроз. Мы предоставляем актуальные знания об эффективных стратегиях обнаружения сложных угроз, реагирования на инциденты, реверс инжиниринга, а также разработки безопасных решений, основанные на внушительном опыте экспертов «Лаборатории Касперского».



## Кому подойдут тренинги xTraining?

- ИБ-специалисты
- Руководители SOC
- Консультанты по кибербезопасности
- Специалисты по активному поиску угроз
- Специалисты по реверс-инжинирингу вредоносного ПО
- Эксперты по безопасной разработке ПО
- Госучреждения и подразделения CERT
- Вузы и исследовательские институты

## Преподаватели Kaspersky xTraining



**Игорь Кузнецов,**  
Директор Глобального центра исследования и анализа угроз (GReAT)



**Айман Шаабан,**  
Руководитель группы цифровой криминалистики и реагирования на инциденты



**Дмитрий Шмойлов,**  
Руководитель отдела безопасности программного обеспечения



**Татьяна Шишкова,**  
Ведущий исследователь угроз информационной безопасности Глобального центра исследования и анализа угроз (GReAT)

# Реверс-инжиниринг

## Реверс-инжиниринг для начинающих **Базовый уровень**

- Получите базовые знания по анализу вредоносного ПО.
- Ознакомьтесь с основными инструкциями ассемблера Intel.
- Изучите различные соглашения о вызовах (stdcall, fastcall) и типы памяти (автоматический, динамический, статический).
- Выполните анализ исполняемых файлов, созданных различными компиляторами, чтобы лучше ориентироваться в более сложных компиляторах.
- Подготовьтесь к следующему уровню курса по реверс-инжинирингу.

## Реверс-инжиниринг вредоносного ПО для мобильных устройств **Средний уровень**

- Научитесь анализировать вредоносное ПО для мобильных устройств (с образцами для Android/iOS).
- Освойте расширенный статический (поверхностный) анализ: разрешения, строки, сигнатуры, файлы ресурсов, декомпиляция байткода Dalvik.
- Узнайте, как проводить статический анализ нативных библиотек для Android и iOS с помощью Ghidra.
- Освойте продвинутый динамический анализ при помощи динамических инструментов Frida.

## Реверс-инжиниринг таргетированного ПО **Средний уровень**

- Проанализируйте реальные образцы вредоносного ПО, используемого APT-группами.
- Проведите реверс-инжиниринг вредоносных документов и эксплойтов.
- Изучите инструменты реверс-инжиниринга, написанные на разных языках программирования, в том числе скриптовых (C, .NET, Delphi, Powershell, JavaScript, C+), и скомпилированными для архитектур x86 и x64 операционных систем Windows и Linux с помощью различных компиляторов).
- Изучите расширенные возможности инструментов для реверс-инжиниринга, в том числе функции создания скриптов в IDA Pro.

## Техники продвинутого анализа вредоносного ПО **Экспертный уровень**

- Проанализируйте современные сложные образцы кода – от получения исходного артефакта до составления технического описания TTP злоумышленника и IOC.
- Создайте статические дешифраторы для реальных сценариев и проведите последующий глубокий анализ вредоносного кода.
- Проанализируйте документы, с помощью которых злоумышленники обычно доставляют полезную нагрузку, и узнайте, как их извлекать.
- Узнайте, как точно и эффективно оценить ущерб и ликвидировать последствия инцидента.

## Продвинутый реверс-инжиниринг с Ghidra **Экспертный уровень**

- Ознакомьтесь с процессом настройки Ghidra и сборки ее актуальной версии из исходного кода.
- Рассмотрите типичный рабочий процесс анализа вредоносного ПО с помощью Ghidra.
- Получите четкое представление о том, как работать с типами и структурами данных в Ghidra.
- Научитесь определять код библиотеки среды выполнения с помощью Ghidra.
- Узнайте, как с помощью скриптов Ghidra автоматизировать задачи реверс-инжиниринга.
- Узнайте, как расширить возможности Ghidra с помощью среды разработки Eclipse.

# Активный поиск угроз

## Поиск APT-угроз с помощью YARA **Базовый уровень**

- Научитесь писать четкие эффективные YARA-правила, в том числе с использованием генераторов YARA-правил для экономии времени и сил.
- Освойте тестирование YARA-правил на ложные срабатывания, которые могут исказить результат.
- Выявляйте скрытые образцы вредоносного ПО в инфраструктуре и на облачных платформах.
- Используйте внешние модули в YARA для еще более эффективного поиска угроз.
- Узнайте секреты поиска аномалий.
- Проверьте знания на реальных примерах, таких как атаки групп BlueTraveller и DiplomaticDuck.

## Мониторинг ИБ и поиск угроз **Средний уровень**

- Изучите структуру центра мониторинга и реагирования в рамках сервисов по защите безопасности.
- Научитесь планировать и организовывать мониторинг безопасности в компании.
- Научитесь использовать различные источники данных об угрозах для обнаружения новых продвинутых угроз.
- Научитесь выявлять и расследовать вредоносную активность в инфраструктурах на базе Windows и Linux с учетом TTP злоумышленников.
- Изучите инфраструктуру поиска угроз на основе ELK (Elasticsearch, Logstash, Kibana).

## Использование Suricata для поиска угроз и реагирования на инциденты

### **Базовый уровень**

- Познакомьтесь с NIDS и методами его использования.
- Освойте навыки написания правила Suricata для различных протоколов.
- Изучите способы оптимизации Suricata правил.
- Углубите знания об основных видах сетевых атак.
- Научитесь проводить анализ подозрительного трафика и распознавать аномалии трафика.
- Узнайте, как определить и минимизировать ложные срабатывания.
- Научитесь использовать Suricata для поиска угроз.

# Реагирование на инциденты

## Реагирование на инциденты в Windows **Средний уровень**

- Изучите последовательность и содержание этапов реагирования на инциденты.
- Изучите способы выявления киберинцидентов и реагирования на них.
- Освойте различные методы атак и анатомию целевых атак на примере цепочки поражения.
- Научитесь отличать APT-угрозы от других типов угроз.
- Повысьте качество создаваемых индикаторов компрометации (IoC).
- Научитесь проводить анализ пораженных машин в режиме реального времени.
- Освойте навыки криминалистического анализа сетевого трафика и памяти.
- Научитесь проводить анализ файлов журналов с помощью регулярных выражений и ELK.

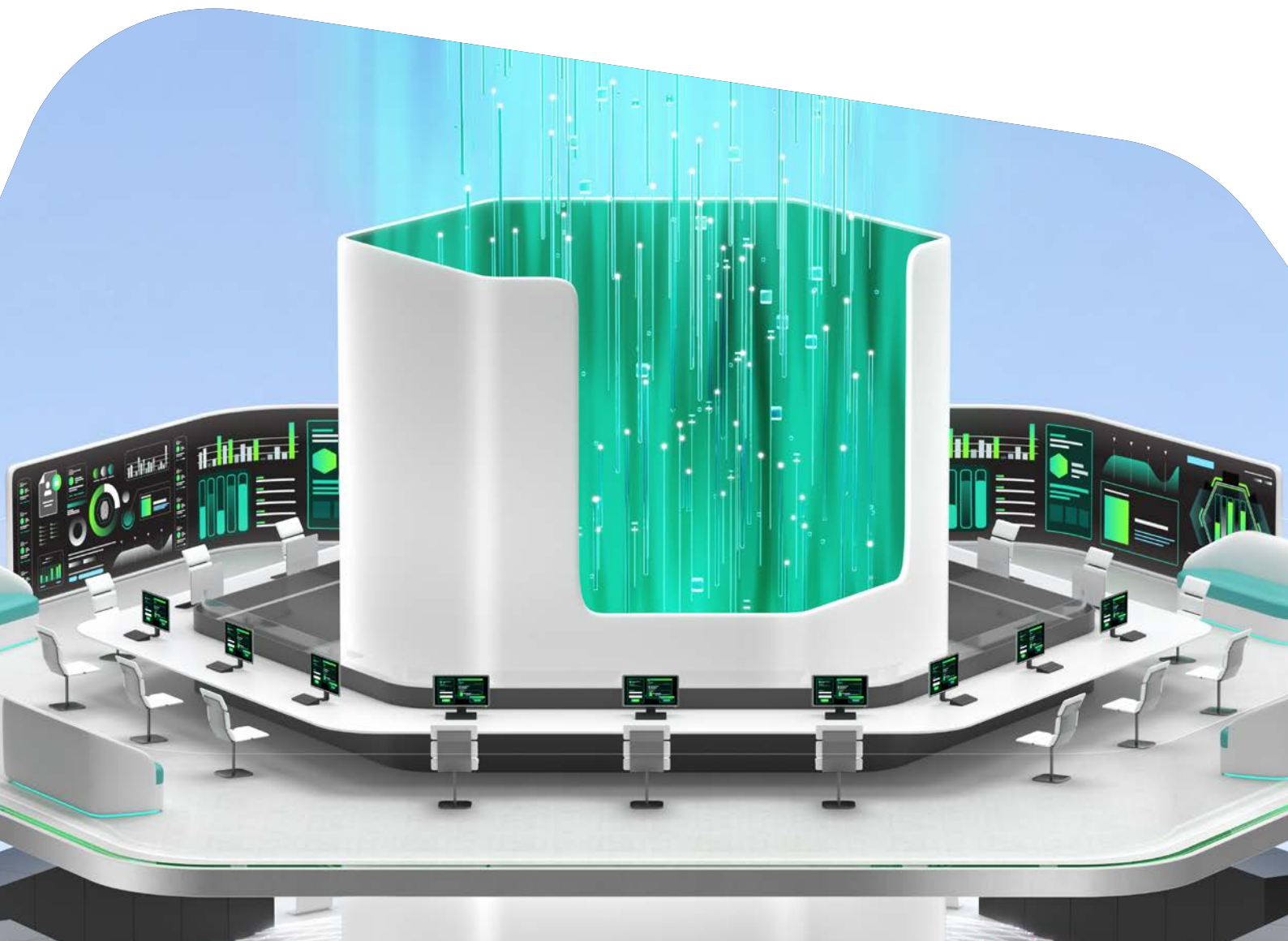
## Цифровая криминалистика в Windows Средний уровень

- Изучите методы обнаружения различных цифровых улик и управления ими в рамках криминалистической экспертизы.
- Освойте основные инструменты и методы цифровой криминалистики.
- Научитесь находить следы вредоносных действий, связанные с инцидентами, в артефактах Microsoft Windows.
- Научитесь проводить эффективный криминалистический анализ памяти, истории браузера и электронной почты.
- Научитесь восстанавливать сценарий инцидента используя временные метки из различных артефактов Windows.

## Разработка безопасных решений

### Безопасная разработка программного обеспечения Средний уровень

- Изучите основные инструменты и практики безопасной разработки, а также принципы реализации жизненного цикла безопасной разработки ПО в компании.
- Углубите знания о подходах к моделированию угроз и проектированию архитектуры продуктов с учетом требований безопасности.
- Научитесь интегрировать лучшие практики и инструменты OWASP в процессы разработки для повышения безопасности создаваемых продуктов.
- Погрузитесь в практики безопасного программирования на C/C++ и получите практические рекомендации по повышению безопасности кода.



# Узнать больше об xTraining

[Подробнее](#)

[Связаться](#)