Первая линия кибероборонны. Курс для ИТ-специалистов общего профиля

Онлайн-курс по кибербезопасности для ИТ-специалистов (CITO)

Бесплатная пробная версия
cito.kaspersky.com

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Cybersecurity for IT Online

Онлайн-курс по кибербезопасности для ИТ-специалистов (CITO)

Интерактивный обучающий курс для ИТ-специалистов общего профиля, который поможет освоить навыки реагирования на инциденты первого уровня

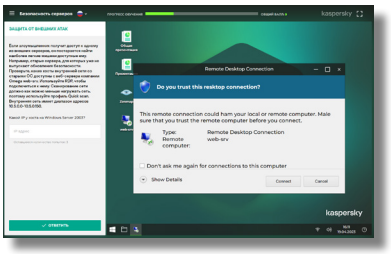
Создание надежной системы корпоративной кибербезопасности невозможно без систематического обучения сотрудников. Большинство компаний проводят обучение и подготовку в области кибербезопасности на двух уровнях: экспертное обучение для групп ИТ-безопасности и повышение осведомленности о безопасности для сотрудников, не связанных с ИТ. «Лаборатория Касперского» предлагает полный набор продуктов для этих уровней обучения. Однако чего-то не хватает. Для отделов ИТ, службы поддержки и других технически подготовленных сотрудников недостаточно стандартных программ повышения осведомленности. В то же время нет необходимости делать из них экспертов по кибербезопасности: это затратно и требует много времени.

Формат тренинга

Тренинг проходит в режиме онлайн. Для обучения требуется только доступ в интернет и браузер Chrome, установленный на компьютере. Каждый из 6 модулей содержит краткую теоретическую часть, практические рекомендации и от 4 до 10 упражнений для отработки конкретных навыков использования инструментов и программ для обеспечения ИТ-безопасности в повседневной работе.

Курс рассчитан примерно на год. Рекомендуется выполнять по одному упражнению в неделю. Выполнение одного упражнения занимает от 5 до 45 минут.

Текущая версия тренинга предназначена для использования в корпоративной среде Windows.



Формат проведения тренинга:
онлайн, в облаке или в формате SCORM.

Первая линия защиты при реагировании на инциденты

«Лаборатория Касперского» запускает первый на рынке онлайн-тренинг для корпоративных ИТ-специалистов широкого профиля. Он состоит из 6 модулей*:

- Вредоносные программы.
- Потенциально нежелательные программы и файлы.
- Основы расследования инцидентов.
- Реагирование на фишинговые атаки.
- Безопасность сервера.
- Безопасность Active Directory.

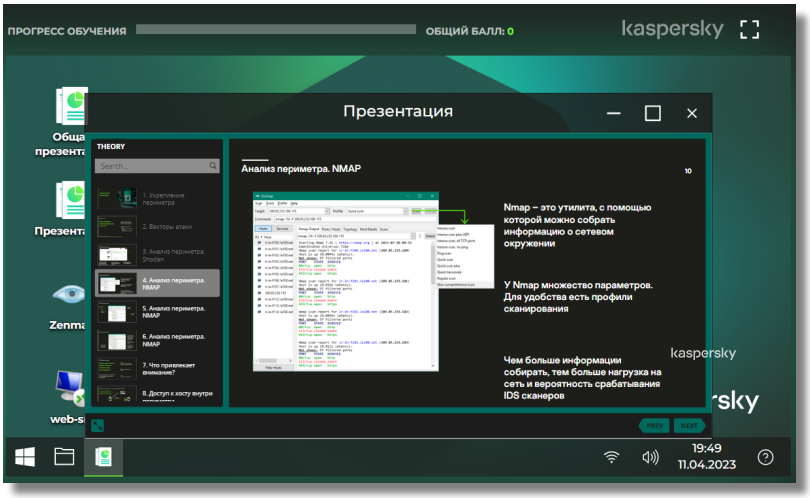
В результате обучения ИТ-специалисты приобретают практические навыки распознавания возможных сценариев атак в, казалось бы, безобидных инцидентах, а также знакомятся со способами сбора данных об инцидентах для передачи в службу ИТ-безопасности. Они также могут увлечься поиском признаков вредоносной активности, в результате чего все сотрудники ИТ-отдела смогут выступать в роли первой линии защиты.

Почему тренинг CITO эффективен?

- Интерактивный – стимуляция реальных процессов осуществляется без риска для компьютера.
- Прикладной – навыки и знания формируются на практике.
- Интуитивно понятный процесс обучения – удобная навигация и подсказки.
- Общий – покрывает все основные темы и проблемы ИТ-безопасности, с которыми сотрудники ИТ-отделов сталкиваются в повседневной работе.

Процесс обучения

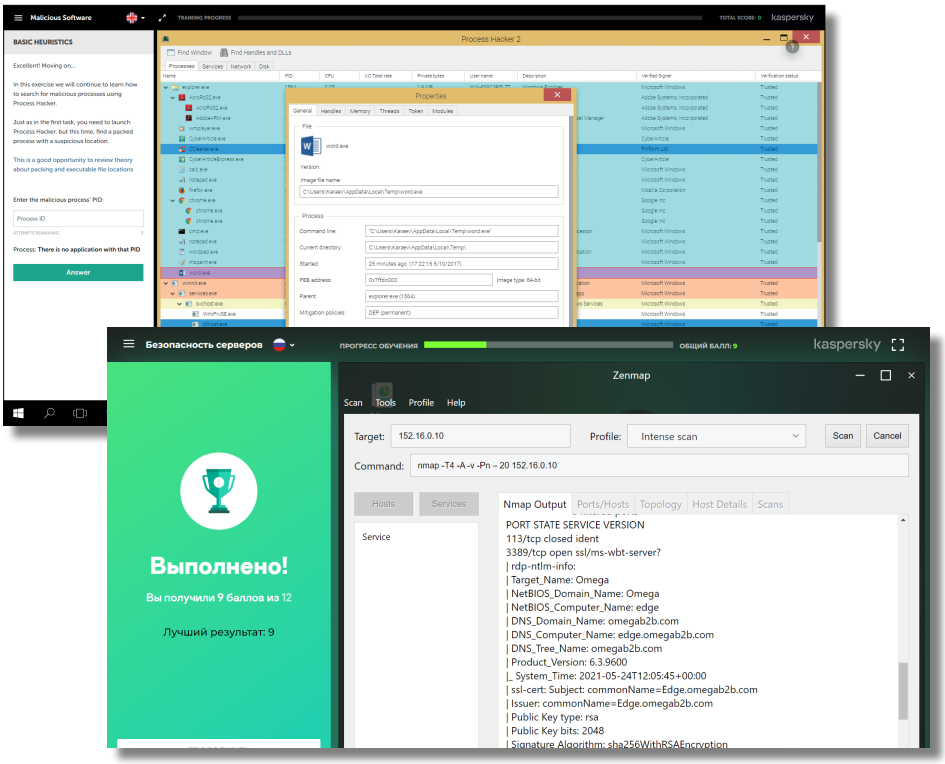
Каждый блок упражнений состоит из двух частей: теоретической и практической. Задания имитируют реальные процессы, описанные в теоретической части.



*Обновленный список тем и понятий ищите на cito.kaspersky.com

Когда вы закончите работу над уроком, завершите задание.

Если вы справились с заданием, вы сможете перейти к следующему блоку упражнений. Если не все получилось, можно воспользоваться подсказками или перечитать материал урока, чтобы освежить свои знания.



Сертификаты

По завершении каждого модуля сотрудникам выдаются персональные сертификаты.

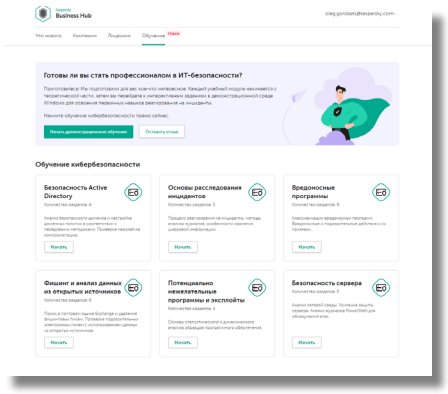
Для кого этот тренинг?

Тренинг рекомендуется для всех ИТ-специалистов компании, особенно для сотрудников службы поддержки и системных администраторов. Он также будет полезен большинству сотрудников отдела ИТ-безопасности, не являющихся экспертами.

Темы тренинга и результаты обучения

Название модуля	Целевая аудитория	Приобретаемые знания	Дополнительная информация	Приобретенные навыки	Упражнения
Вредоносные программы	Пользователи с правами администратора на серверах и рабочих станциях	Техники и классификация вредоносных программ Поведение и признаки вредоносных и подозрительных программ Основы эвристического анализа	Вредоносные программы могут находиться в любом месте на компьютере Вредоносные программы могут совершать кражу данных различными нетривиальными способами Обо всех подозрительных моментах и возможных инцидентах необходимо сообщать службе безопасности	Проверка наличия или отсутствия инцидента, вызванного вредоносными программами	Использование инструментов ProcessHacker, Autoruns, Fiddler, Gmer для обнаружения вредоносных программ

Название модуля	Целевая аудитория	Приобретаемые знания	Дополнительная информация	Приобретенные навыки	Упражнения
Потенциально нежелательные программы и файлы	Пользователи с правами на установку дополнительных программ и пользователи, часто оценивающие или открывающие файлы, полученные извне	Основы статистического и динамического анализа образцов программ и подозрительных документов	Документы (pdf, docx) могут содержать эксплойты Неподписанные файлы могут содержать вредоносные или потенциально опасные программы Все неподписанные исполняемые файлы должны проверяться на вероятное заражение Цифровая подпись не гарантирует того, что файл не содержит вредоносных функций	Работа с мониторами системных событий и изолированной средой (песочницей) Использование статистических механизмов Удаление потенциально нежелательных программ	Статический (сигнатурный) и статистический (VirusTotal) анализ образцов программ Использование procmon для выявления эксплойтов и вредоносного поведения программ Анализ файлов с помощью песочницы Cuckoo Создание скриптов для удаления вредоносных программ с помощью AVZ
Основы расследования инцидентов	Сотрудники ИТ-отделов, участвующие в судебной экспертизе и реагировании на инциденты под руководством группы обеспечения безопасности	Процесс реагирования на инциденты Методы анализа журналов Особенности хранения цифровой информации	Если вы подозреваете, что произошел киберинцидент, немедленно сообщите об этом группе обеспечения безопасности и соберите цифровые доказательства Анализ инцидента следует проводить под руководством и в сотрудничестве с группой обеспечения безопасности	Сбор цифровых доказательств Анализ сетевого трафика NetFlow Анализ хронологии событий Анализ журналов событий	Сбор переменных и постоянных данных (FTK-imager) Анализ журналов с целью поиска источника и звеньев атаки (Eventlog Explorer) Анализ распространения атаки с помощью анализа трафика NetFlow (Ntop) Анализ диска с помощью Autopsy
Фишинг и анализ данных из открытых источников (OSINT)	Сотрудники ИТ-отделов, участвующие в судебной экспертизе и реагировании на инциденты	Современные методы фишинга Методы анализа заголовков сообщений электронной почты	Фишинг может быть очень изощренным, что затрудняет его обнаружение, однако его всегда можно обнаружить при расследовании вручную Фишинговые письма необходимо удалять из почтовых ящиков пользователей	Анализ и удаление фишинговых писем из почтовых ящиков пользователей Анализ информации из открытых источников для понимания того, что известно злоумышленникам о вашей компании	Поиск и удаление фишинговых писем из почтового ящика Microsoft Exchange Использование Recon-ng для поиска информации в открытых источниках
Безопасность сервера	Администраторы сервера	Анализ сетевого окружения Усиление защиты сервера Анализ журналов PowerShell с целью обнаружения атак	Компрометация сетевого периметра – это один из основных векторов атак. Невозможно закрыть все уязвимости, однако, чтобы максимально усложнить атаку, необходимо уменьшить поверхность атаки. Даже если это не остановит злоумышленников, это даст вам время для обнаружения атаки.	Поиск уязвимых и нестандартных сетевых сервисов Настройка системы в соответствии с принципом «запрет по умолчанию» Поиск признаков атаки в журналах PowerShell	Использование Nmap для поиска уязвимых сетевых сервисов Настройка политик ограничения использования программ для управления программами и настройка брандмауэра Windows для контроля сети Анализ событий с помощью Event Log Explorer
Безопасность Active Directory	Администраторы Active Directory	Использование API для проверки паролей по базе данных скомпрометированных паролей Настройка доменных политик в соответствии с рекомендациями Методы анализа безопасности доменов Active Directory	Установленные по умолчанию параметры конфигурации Active Directory не оптимальны с точки зрения безопасности Злоумышленники могут повысить свои привилегии разными способами Следует изучить рекомендации по безопасности и использовать инструменты, обеспечивающие лучшую видимость Active Directory	Безопасная проверка хэшей паролей по базе данных Поиск несоответствий между рекомендованными и фактическими доменными политиками Оценка уровня безопасности параметров Active Directory	Использование функции Have I Been Pwned? API для поиска по базе скомпрометированных паролей Использование анализатора политик для сравнения текущих доменных политик с рекомендованными Работа с отчетами Ping Castle



Интеграция с Kaspersky Endpoint Security Cloud

Совершенствуйте свои навыки в области кибербезопасности и получайте максимальную выгоду от использования специализированных защитных продуктов с помощью тренинга CITO, доступного для пользователей KES Cloud Pro прямо через Kaspersky Business Hub .

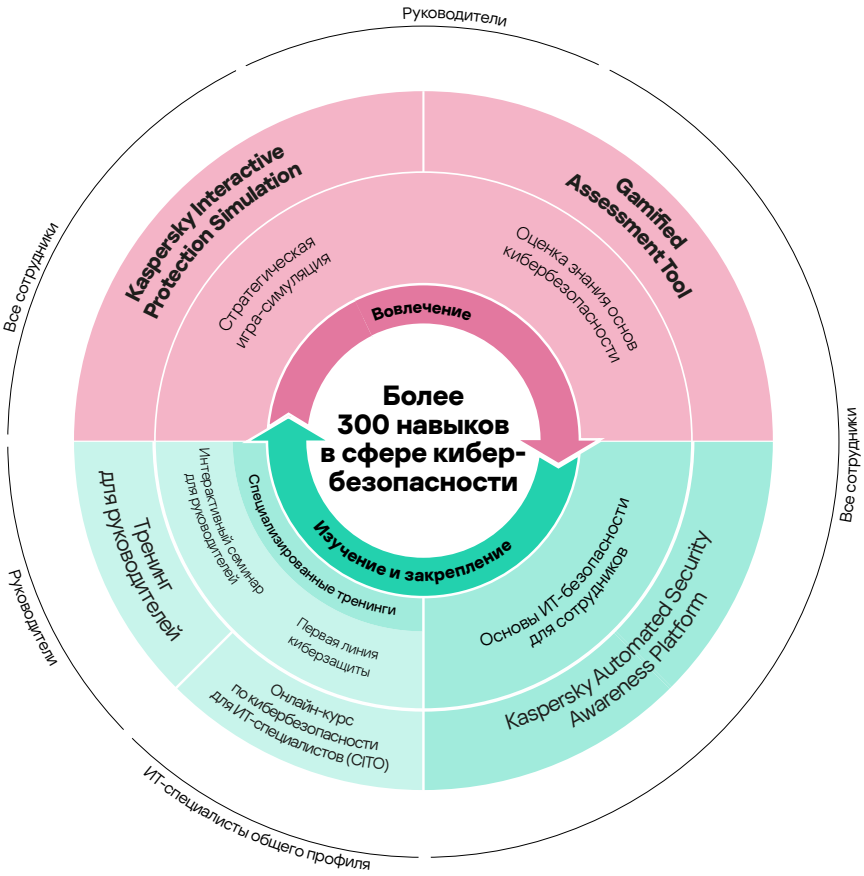
Kaspersky Security Awareness – новый подход к обучению в сфере ИТ-безопасности

Единое гибкое обучающее решение для всех

Комплекс тренингов Kaspersky Security Awareness – это проверенное и эффективное решение, которое давно и успешно зарекомендовало себя в мире. Предприятия разного размера **более чем в 75 странах мира уже воспользовались этим решением для обучения более миллиона своих сотрудников**. В этом решении соединился более чем 25-летний опыт «Лаборатории Касперского» в области кибербезопасности с богатейшим опытом Kaspersky Academy в области обучения людей.

Комплекс состоит из увлекательных учебных курсов, которые помогут повысить киберграмотность сотрудников любого уровня и усилить их роль в общей структуре кибербезопасности предприятия.

Поскольку для формирования устойчивого кибербезопасного поведения требуется время, наш подход подразумевает непрерывный и многокомпонентный цикл получения знаний и навыков. Игровая форма обучения помогает заинтересовать высших руководителей компании и превратить их в главных сторонников и инициаторов формирования культуры кибербезопасного поведения. Оценка результатов игры позволяет выявить пробелы в знаниях сотрудников и мотивировать их к дальнейшему обучению, а онлайн-платформы и симуляторы помогают им приобретать и совершенствовать необходимые навыки.



Ключевые особенности программы

Глубокие знания в области кибербезопасности
Более чем за 25 лет работы в области кибербезопасности мы сформировали набор навыков, который лег в основу наших продуктов.

Обучение, меняющее поведение сотрудников на всех должностях в компании
Игровое обучение обеспечивает вовлечение и мотивацию, а учебные платформы помогают усвоить набор навыков кибербезопасности и гарантируют, что со временем полученные навыки не забудутся.

Корпоративная кибербезопасность: www.kaspersky.ru/enterprise
Kaspersky Security Awareness: www.kaspersky.ru/awareness
Онлайн-курс по кибербезопасности для ИТ-специалистов (CITO): cito.kaspersky.com

www.kaspersky.ru

kaspersky **АКТИВИРУЙ БУДУЩЕЕ**