

СЕРВИСЫ KASPERSKY SECURITY INTELLIGENCE

Тренинги по кибербезопасности

ТРЕНИНГИ ПО КИБЕРБЕЗОПАСНОСТИ

В рамках этих инновационных образовательных программ «Лаборатория Касперского» делится своими экспертными знаниями и опытом в сфере информационной безопасности, а также уникальными данными о киберугрозах.

Для современных предприятий, которые сталкиваются с непрерывно растущим объемом постоянно меняющихся киберугроз, чрезвычайно важно быть в курсе главных проблем IT-безопасности. Эффективная корпоративная стратегия по защите от угроз и минимизации последствий кибератак немыслима без развития у специалистов навыков работы с передовыми технологиями IT-безопасности. При этом все сотрудники без исключения должны владеть базовыми знаниями о киберугрозах и навыками безопасной работы.

Курсы «Лаборатории Касперского» по кибербезопасности ориентированы на компании, которые стремятся защитить свою инфраструктуру и интеллектуальную собственность.

ТРЕНИНГИ ПО КИБЕРБЕЗОПАСНОСТИ

Программа повышения осведомленности о киберугрозах

Программа экспертного обучения в области ИБ

КУРСЫ

ОБУЧЕНИЕ СОТРУДНИКОВ	ОБУЧЕНИЕ ЭКСПЕРТОВ	
Сотрудники	Уровень 1, базовый	
ОНЛАЙН-ПЛАТФОРМА	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Базовые знания в области IT	ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ПРАКТИЧЕСКИЙ КУРС Базовые знания в области IT
Линейные руководители	Уровень 2, средний	
ИГРОВОЙ ФОРМАТ CYBERSAFETY	ЦИФРОВАЯ КРИМИНАЛИСТИКА Требуются навыки системного администрирования	АНАЛИЗ И ОБРАТНАЯ РАЗРАБОТКА ВРЕДНОСНОГО ПО Требуются навыки программирования
Руководители организаций	Уровень 3, экспертный	
ОЦЕНКА УРОВНЯ ОСВЕДОМЛЕННОСТИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ	ЦИФРОВАЯ КРИМИНАЛИСТИКА (ПРОФЕССИОНАЛЬНЫЙ УРОВЕНЬ) Требуются экспертные навыки системного администрирования	АНАЛИЗ И ОБРАТНАЯ РАЗРАБОТКА ВРЕДНОСНОГО ПО (ПРОФЕССИОНАЛЬНЫЙ УРОВЕНЬ) Требуются навыки программирования на языке ассемблер

ПРОГРАММА ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ О КИБЕРУГРОЗАХ

Интерактивные учебные онлайн-модули и обучающие игры по кибербезопасности внутри компании предназначены для всех сотрудников, которые пользуются компьютерами или мобильными устройствами.

80% всех инцидентов кибербезопасности происходят по причине человеческого фактора. Компании тратят миллионы, чтобы рассказать сотрудникам о проблемах информационной безопасности (ИБ) и научить их правильному поведению, но мало кто из руководителей соответствующих департаментов доволен результатами. Почему так получается?

Большинство тренингов по кибербезопасности продолжаются слишком долго, переполнены техническими подробностями и рисуют слишком мрачную картину мира. Такие тренинги в результате могут оказаться неэффективными.

Поэтому сегодня организации ищут комплексный подход, стимулирующий правильное поведение сотрудников (например, при помощи разработки соответствующей корпоративной культуры). Только с его помощью инвестиции в программы повышения осведомленности наконец-то начнут приносить весомую и измеримую пользу.

Курсы «Лаборатории Касперского» эффективны благодаря следующим факторам.

- Изменение поведения. Мы поощряем стремление каждого сотрудника к безопасной работе, создавая корпоративную среду, в которой каждый соблюдает правила кибербезопасности, потому что так поступают все остальные.
- Сочетание мотивирующих приемов, обучения в игровой форме, имитации атак и подробных интерактивных тренингов, формирующих навыки кибербезопасности.

ПРИНЦИПЫ РАБОТЫ

Глубина охвата и ясность изложения

Тренинг затрагивает широкий круг вопросов безопасности, освещая как причины утечки данных и особенности вирусных атак через интернет, так и принципы безопасной работы в социальных сетях. А простые упражнения помогают усваивать материал.

Благодаря использованию разных методик (работа в группах, интерактивные модули, забавные комиксы и обучение в игровой форме) обучение проходит легко и увлекательно.

Постоянная мотивация

Мы создаем условия для обучения в игровой форме, поддерживая соревновательный дух, а затем в течение года закрепляем материал, моделируя атаки через интернет и проводя оценочные и образовательные активности.

Новый взгляд на ситуацию

Мы рассказываем, что мишенями киберпреступников чаще всего оказываются не машины, а живые люди, и показываем, как соблюдение правил безопасности помогает защитить себя и свое рабочее место от кибератак.

Формирование корпоративной культуры кибербезопасности

Мы готовим руководителей к роли лидеров в борьбе за безопасность на рабочем месте. Только личным примером руководства можно сформировать корпоративную среду, в которой кибербезопасность воспринимается естественно, а не как набор правил, выдуманных IT-специалистами.

Позитивный подход и совместная работа

Мы показываем, как соблюдение правил безопасности повышает эффективность работы всей организации и помогает улучшить сотрудничество с другими подразделениями, в том числе с IT-департаментом.

Измеримый эффект

Мы предоставляем инструменты для измерения навыков сотрудников и проводим оценку на корпоративном уровне, анализируя отношение персонала к кибербезопасности в повседневной работе.

ПРОГРАММА ЭКСПЕРТНОГО ОБУЧЕНИЯ В ОБЛАСТИ ИБ

Эти курсы охватывают самые разные темы и подходы, связанные с обеспечением IT-безопасности, и подразделяются на несколько категорий – от базового до экспертного уровня. Все учебные курсы проводятся в региональных офисах «Лаборатории Касперского» либо на территории заказчика.

Курсы включают как теоретические, так и практические лабораторные занятия. По завершении каждого курса все участники могут пройти тестирование и подтвердить свой уровень знаний.

УРОВНИ: БАЗОВЫЙ, СРЕДНИЙ И ЭКСПЕРТНЫЙ

Программа охватывает широкий круг вопросов: от основ информационной безопасности до цифровой криминалистики и анализа вредоносных программ. Она призвана помочь сотрудникам расширить свои знания в трех важных областях:

- основы IT-безопасности;
- цифровая криминалистика и реагирование на инциденты;
- анализ и обратная разработка вредоносного ПО.

ПРЕИМУЩЕСТВА ДЛЯ КЛИЕНТОВ

УРОВЕНЬ 1

Основы информационной безопасности

Администраторы и руководители, отвечающие за информационные технологии и защиту от угроз, получают базовые представления о новейших мерах по обеспечению информационной безопасности.

УРОВЕНЬ 1

Основы информационной безопасности с практическими занятиями

Углубленное изучение вопросов безопасности на практических занятиях с применением современных инструментов.

УРОВНИ 2 и 3

Цифровая криминалистика

Повышение профессионального уровня штатных специалистов, отвечающих за криминалистический анализ и реагирование на инциденты компьютерной безопасности.

УРОВНИ 2 и 3

Анализ и обратная разработка вредоносного ПО

Повышение профессионального уровня штатных специалистов, отвечающих за анализ и обратную разработку вредоносных программ.

ПРАКТИЧЕСКИЙ ОПЫТ

Работа вместе с экспертами мирового класса вдохновит участников и позволит приобрести реальный опыт обнаружения и предотвращения киберпреступлений с помощью новейших технологий.

ОПИСАНИЕ ПРОГРАММЫ

Темы	Продолжительность	Навыки
УРОВЕНЬ 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ		
<ul style="list-style-type: none"> Обзор черного рынка киберугроз и хакерских услуг Спам, фишинг, безопасность электронной почты Технологии защиты от мошенничества Эксплойты, угрозы для мобильных устройств и комплексные таргетированные угрозы Основы расследования инцидентов с помощью общедоступных веб-инструментов Безопасность рабочего места 	2 дня	<ul style="list-style-type: none"> Обнаружение инцидентов безопасности и выбор способа их разрешения Снижение нагрузки на отделы информационной безопасности Повышение безопасности рабочего места каждого сотрудника с помощью дополнительных средств Проведение простых расследований Анализ фишинговых писем Распознавание зараженных и поддельных веб-сайтов
УРОВЕНЬ 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПРАКТИЧЕСКИМИ ЗАНЯТИЯМИ		
<ul style="list-style-type: none"> Основы ИБ Использование общедоступных источников для сбора и анализа информации Безопасность корпоративной сети Безопасность приложений и защита от эксплойтов DDoS-атаки Безопасность беспроводных сетей и мобильных сетей Угрозы для банкинга и мобильных устройств Реагирование на инциденты безопасности в облачной и виртуальной среде 	5 дней	<ul style="list-style-type: none"> Простые расследования с использованием общедоступных ресурсов, специализированных поисковых систем и социальных сетей Создание периметра безопасности сети Базовые навыки тестирования на проникновение Изучение трафика для обнаружения атак различного типа Соблюдение безопасности при разработке ПО Обнаружение инъекций вредоносного кода Проведение базовых процедур цифровой криминалистики и анализа вредоносного ПО
УРОВЕНЬ 2. ОБЩИЕ ВОПРОСЫ ЦИФРОВОЙ КРИМИНАЛИСТИКИ		
<ul style="list-style-type: none"> Введение в цифровую криминалистику Оперативное реагирование и сбор цифровых улик Внутренняя структура реестра Windows Анализ артефактов в Windows Криминалистический анализ браузера Анализ электронной почты 	5 дней	<ul style="list-style-type: none"> Организация лаборатории цифровой криминалистики Сбор цифровых улик и порядок обращения с ними Воссоздание хронологической картины инцидента с помощью меток времени Выявление следов вторжения посредством анализа артефактов в ОС Windows Анализ истории браузера и электронной почты Умение применять инструменты цифровой криминалистики
УРОВЕНЬ 2. ОСНОВЫ АНАЛИЗА И ОБРАТНОЙ РАЗРАБОТКИ ВРЕДНОСНОГО ПО		
<ul style="list-style-type: none"> Цели и методы анализа и обратной разработки вредоносного ПО Внутреннее устройство ОС Windows, исполняемые файлы, ассемблер x86 Базовые методы статического анализа (извлечение строк, анализ импортов, анализ точек входа PE-файла, автоматическая распаковка и т. д.) Базовые методы динамического анализа (отладка, инструменты мониторинга, перехват трафика и т. д.) Анализ файлов .NET, Visual Basic®, Win64 Методы анализа сценариев и программ, отличных от PE-файлов (Batchfiles, Autoit, Python, Jscript®, JavaScript, VBScript) 	5 дней	<ul style="list-style-type: none"> Построение безопасной среды для анализа вредоносных программ: развертывание «песочницы» и всех необходимых инструментов Понимание принципов исполнения программ в ОС Windows Распаковка, отладка и анализ вредоносного объекта, определение его функций Обнаружение вредоносных сайтов путем анализа вредоносных скриптов Проведение экспресс-анализа вредоносного ПО
УРОВЕНЬ 3. ЭКСПЕРТНАЯ ЦИФРОВАЯ КРИМИНАЛИСТИКА		
<ul style="list-style-type: none"> Экспертная криминалистика в ОС Windows Восстановление данных Сетевая и облачная криминалистика Криминалистический анализ дампов памяти Хронологический анализ Практическая криминалистика реальных целевых атак 	5 дней	<ul style="list-style-type: none"> Глубокий анализ файловой системы Восстановление удаленных файлов Анализ сетевого трафика Выявление вредоносных программ по дампам памяти Восстановление хронологии инцидента
УРОВЕНЬ 3. АНАЛИЗ И ОБРАТНАЯ РАЗРАБОТКА КОМПЛЕКСНОГО ВРЕДНОСНОГО ПО		
<ul style="list-style-type: none"> Цели и методы анализа и обратной разработки вредоносного ПО Методы расширенного статического и динамического анализа (ручная распаковка) Методы деобфускации Анализ руткитов и буткитов Анализ эксплойтов (файлы pdf, doc, swf и др.) Анализ вредоносного ПО для Android™, Linux®, Mac OS® 	5 дней	<ul style="list-style-type: none"> Использование передовых методов обратной разработки Распознавание методов защиты от обратной разработки (обфускация, защита от отладки) Расширенный анализ руткитов и буткитов Анализ шелл-кода эксплойтов, внедренного в различные виды файлов Анализ вредоносного ПО для сред, отличных от Windows

АО «Лаборатория Касперского» | Решения для бизнеса: | +7 (495) 737-34-12
www.kaspersky.ru | www.kaspersky.ru/enterprise | sales@kaspersky.com

© АО «Лаборатория Касперского», 2016. Все права защищены. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей. Windows, Visual Basic, Jscript – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах. Java Script – зарегистрированный товарный знак Oracle Corporation и/или ее аффилированных компаний. Android – товарный знак Google, Inc. Linux – товарный знак Linus Torvalds, зарегистрированный в США и других странах. Mac OS – зарегистрированный товарный знак Apple, Inc.

