



---

**Программы  
повышения  
осведомленности  
для всех уровней  
организации**

2020

# **Kaspersky Security Awareness**

**kaspersky**

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

# Навыки киберграмотности — важнейший фактор обеспечения кибербезопасности

Более 80% всех инцидентов кибербезопасности происходят из-за человеческого фактора. Предприятия тратят огромные средства, восстанавливая ресурсы после нарушений безопасности, вызванных действиями сотрудников. Однако традиционные программы повышения осведомленности, призванные предотвращать такие инциденты, недостаточно эффективны. Обычно они не вдохновляют участников и не позволяют сформировать у них требуемое поведение.

Люди — самое слабое звено в системе безопасности:

**52%** компаний считают, что сотрудники — это самая большая угроза кибербезопасности\*

**60%** сотрудников хранят конфиденциальные данные на корпоративных устройствах (в т. ч. финансовую информацию, электронную почту и пр.)\*\*

**30%** сотрудников признают, что сообщают коллегам учетные данные своего рабочего компьютера\*\*

**23%** организаций не имеют правил или политик безопасности хранения корпоративных данных\*\*

## Решение

Используйте наши возможности для повышения киберграмотности сотрудников и сделайте их первой линией киберзащиты.

## Почему клиентам не нравятся текущие программы повышения осведомленности?

### Они не эффективны

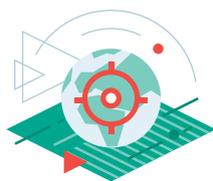
- Сотрудники воспринимают обучение как скучное и ненужное занятие, слабо связанное с ежедневной работой
- Упор делается на запреты, а не на примеры того, как нужно поступать
- Читать и слушать объяснения — не так эффективно, как участвовать в практических занятиях

### Они дают дополнительную административную нагрузку

- Процесс обучения сложен в управлении и контроле
- Трудно найти новые способы заинтересовать сотрудников обучением и мотивировать их

## Kaspersky Security Awareness — увлекательный процесс, долговременный результат

### Ключевые особенности программ



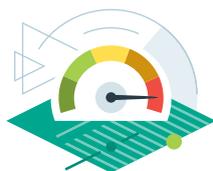
#### Целевые программы, соответствующие должности сотрудника

- Цели сотрудника соответствуют его роли в компании и профилю рисков
- Примеры из реальной жизни и навыки, которые можно немедленно применить
- Упражнения для закрепления знаний



#### Человеко-ориентированный подход

- Структура занятий соответствует естественному способу мышления
- Объяснение правил безопасности идет проактивно и в позитивном ключе
- Сотрудники получают сведения и навыки, которые легко усвоить и закрепить благодаря методикам, учитывающим особенности человеческой памяти



#### Непрерывный процесс с постепенным повышением уровня сложности

- Принцип «от простого к сложному»
- Применение и развитие полученных ранее знаний в новых ситуациях



#### Простота управления и контроля

- Многие программы доступны онлайн
- Автоматическое управление
- Каждому учащемуся по электронной почте автоматически отправляются приглашения и мотивационные письма с индивидуальными рекомендациями

\* Согласно исследованию The cost of a data breach (Ущерб от утечки данных), «Лаборатория Касперского», весна 2018 г.

\*\* Sorting out a Digital Clutter (Наводим порядок в цифровом пространстве), «Лаборатория Касперского», 2019 г.

# Безопасность начинается с осведомленности

С помощью наших программ вы сможете донести правила кибербезопасности до каждого сотрудника: тренинги помогут понять, что такое киберугрозы и как не стать их жертвой.

Сегодня причина большинства инцидентов безопасности в организациях – это человеческий фактор

Человеческий фактор может быть главной киберугрозой для организации, даже если вы применяете традиционные программы повышения осведомленности.

**1 057 000 долл. США на предприятие** – средний финансовый ущерб от утечек данных, произошедших из-за того, что сотрудники использовали IT-ресурсы не по назначению\*

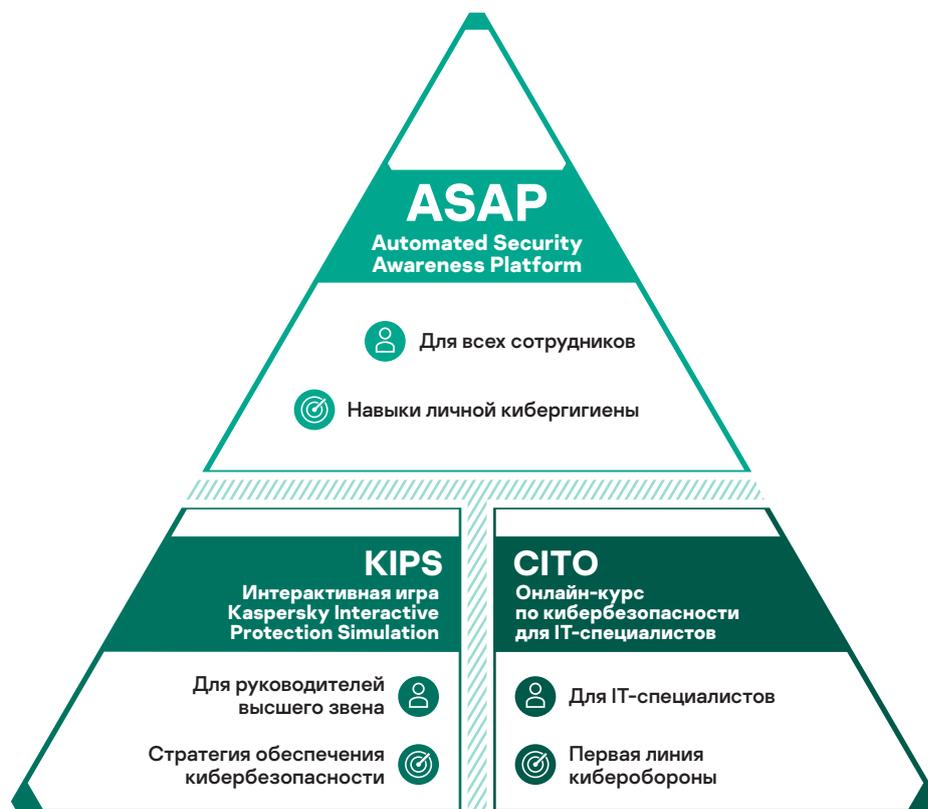
**101 000 долл. США** составляет ущерб от атак с использованием фишинга или социальной инженерии **для каждой компании сегмента малого и среднего бизнеса** (1,3 млн долларов на предприятие)\*\*

До **400** составляет средний ущерб от фишинговых атак **на сотрудника в год\*\*\***

## Тренинги Kaspersky Security Awareness

«Лаборатория Касперского» предлагает тренинги, в которых применяются новейшие образовательные методики. Такой подход меняет поведение пользователей и помогает создать безопасную информационную среду во всей организации.

### Разные форматы обучения для разных уровней организации



\* Отчет On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives (Во что обходятся киберугрозы: рост расходов в сфере информационной безопасности поддерживает цифровую трансформацию), «Лаборатория Касперского», 2018 г.

\*\* Отчет Human factor in IT security: How Employees are Making Businesses Vulnerable from Within (Человеческий фактор в IT-безопасности: как из-за сотрудников бизнес становится уязвимым изнутри), International, июнь 2017 г.

\*\*\* Расчеты основаны на исследовании Ponemon Institute Cost of Phishing and Value of Employee Training (Убытки от фишинга и ценность обучения сотрудников), август 2015 г.

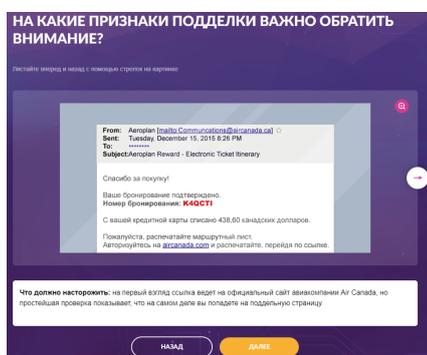
# Описание программ Kaspersky Security Awareness (Kaspersky ASAP)

Kaspersky ASAP предлагает достижимые цели программы, готовый и сбалансированный план занятий, в котором есть задания, относящиеся к реальному рабочему процессу, а также средства составления актуальных отчетов. Решение повышает интерес к получению знаний о кибербезопасности и приносит пользу как сотрудникам, так и компании в целом.

Каждая тема делится на разные уровни, посвященные отработке определенной группы навыков в сфере информационной безопасности. Уровни соответствуют степени опасности угроз. На первом уровне участникам объясняют, как себя вести при прямых и массовых атаках. Проходя уровень за уровнем, они переходят к изучению поведения при целевых атаках и сложных угрозах.

Kaspersky ASAP подходит для поставщиков услуг по управлению безопасностью (MSSP) — инструментами обучения для различных бизнес-подразделений можно управлять из единой учетной записи.

Убедитесь сами, насколько легко можно организовать и контролировать программу повышения киберграмотности. Попробуйте полнофункциональную версию Kaspersky ASAP, зайдя на <https://asap.kaspersky.com/ru/>.



## 1. Платформа Kaspersky Automated Security Awareness Platform

Новый комплексный подход к онлайн-программам повышения осведомленности основан не только на информации, но и на «восприятии паттернов»: он учит сотрудников действовать безопасно даже если они столкнутся с совершенно незнакомой угрозой, но в рамках изученной модели.

### Универсальная программа тренинга

- Широкий набор ключевых тем кибербезопасности, которые доступны на различных уровнях — от начинающего до продвинутого.
- Возможность изучать только те темы и до того уровня, которые необходимы.

### Автоматическое управление

- Запуск платформы занимает всего 10 минут. После этого можно быстро и легко загрузить список пользователей, разделить их на группы и задать для каждой из них уровень в соответствии со сложностью угроз и должностью.
- Затем платформа сама строит план для каждой группы, обеспечивая интервальное прохождение программы. Участники постоянно закрепляют полученные знания благодаря различным форматам (в том числе интерактивным модулям и напоминаниям с основными положениями урока и практическими примерами, присылаемым по электронной почте).

### Подробные отчеты в любое время

- Отслеживание процесса занятий с помощью удобной информационной панели, где отображаются актуальные данные, тенденции и прогнозы.
- Рекомендации по улучшению результатов.

### Ключевые преимущества

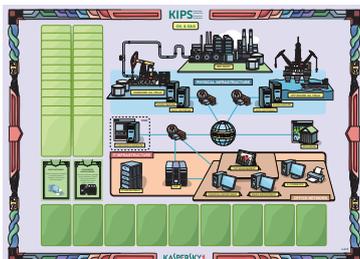
- **Простота благодаря полной автоматизации:** запускать, настраивать и контролировать процесс не составляет труда, а управление полностью автоматизировано и вообще не требует административного участия.
- **Эффективность:** материалы в программе структурированы так, чтобы обеспечивать последовательное интервальное обучение с постоянным закреплением знаний. Методология учитывает особенности человеческой памяти: сотрудники лучше усваивают знания и смогут применять полученные навыки.
- **Гибкое лицензирование:** модель лицензирования из расчета на одного пользователя можно использовать, начиная с 5 лицензий.

\* По состоянию на июль 2019 г.

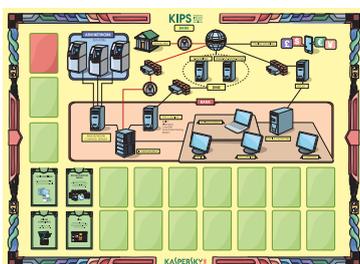
Тренинги KIPS предназначены для руководителей высшего звена, экспертов по бизнес-системам и сотрудников IT-отделов. Тренинг поможет повысить осведомленность о рисках и проблемах безопасности, связанных с современными компьютерными системами.

### Некоторые сценарии применения KIPS

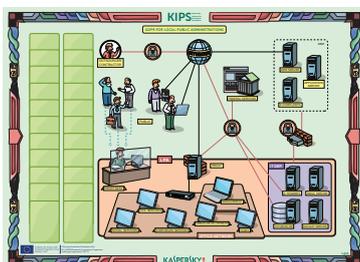
#### Корпорация



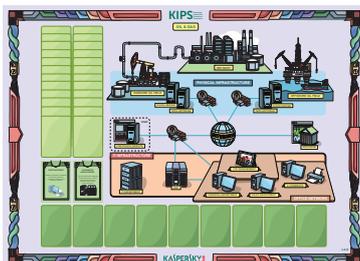
#### Банк



#### Нефтехимия



#### Добыча нефти и газа



#### KIPS в онлайн-формате:

- Идеально подходит для глобальных организаций
- Поддержка до 300 команд одновременно
- Каждая команда может выбрать игровой интерфейс на другом языке
- Преподаватель ведет каждое занятие через WebEx

\* Каждый из сценариев доступен на разном количестве языков.

## 2. Интерактивная игра Kaspersky Interactive Protection Simulation (KIPS) – понимание стратегии в области ИБ

### Что такое KIPS?

KIPS — это командная ролевая игра, имитирующая бизнес-среду, в которой по сценарию участникам предстоит справиться с рядом неожиданных киберугроз. Одновременно игроки должны увеличивать прибыль компании и сохранять ее репутацию.

Цель игры — разработать стратегию кибербезопасности, которая будет эффективна в борьбе против текущих киберугроз и пригодится в будущем.

### Почему игра KIPS так эффективна?

- Увлекательный и действенный подход к обучению кибербезопасности
- Интересный и динамичный игровой процесс (2 часа)
- Развитие навыков работы в команде
- Соревновательный элемент: вы проявляете инициативу, принимаете решения и стремитесь к высокому результату
- Понимание через наглядность: вы видите, к чему приводят ошибки или заблуждения. Вы можете скорректировать свою игру, а затем проанализировать все ошибки в рамках игрового процесса

### Играя в KIPS, вы приобретаете опыт

- Будьте готовы к новым угрозам — узнайте о приемах, которыми пользуются злоумышленники, и об их целях (аналитика угроз)
- Узнайте, как сочетать действия по реагированию на инциденты с задачами по их предотвращению
- Узнайте, что может произойти, вы своевременно не используете меры защиты
- Реагируйте на сигналы тревоги, которые одновременно поступают от систем защиты, IT-отделов и бизнес-отделов

### Сценарии KIPS\*

- **Корпорация:** защита предприятия от программ-вымогателей, APT-угроз, нарушений безопасности автоматизации и других атак.
- **Банк:** защита финансовых учреждений от масштабных APT-угроз, направленных на банкоматы, управляющие серверы и бизнес-системы.
- **Электронные госуслуги / органы местного самоуправления:** защита государственных веб-серверов от атак и эксплойтов.
- **ГЭС / электростанция:** защита промышленных систем управления и критически важной инфраструктуры.
- **Транспорт:** защита пассажиро- и грузоперевозок от ошибок Heartbleed, программ-вымогателей и APT-угроз.
- **Нефтегазовая компания:** понимание того, какой ущерб наносит определенный вид атак — от нарушения работы веб-сайтов до современных программ-вымогателей и комплексных APT-угроз.
- **Нефтехимическое производство:** обеспечение ИБ в новом филиале крупного нефтехимического холдинга, который занимается производством пластиков и другой химической продукции.

Каждый сценарий демонстрирует участникам, насколько важна кибербезопасность для целостности и прибыльности бизнеса, учит определять новые проблемы и угрозы, а также показывает типичные ошибки в организации системы кибербезопасности. При этом коммерческий и ИБ-отделы взаимодействуют друг с другом, что помогает стабилизировать работу и противостоять киберугрозам сообща.

Программа ориентирована на специалистов технической поддержки, специалистов по общей ИТ-безопасности и администраторов локальных служб поддержки

#### Формат

Тренинг полностью проводится в онлайн-режиме: участникам требуется только доступ к интернету или к корпоративной системе управления обучением, а также браузер Chrome.

Каждый из 4 модулей состоит из короткой теоретической части, практических советов и 4–10 упражнений: каждое позволяет отработать определенный практический навык, а также учит использовать инструменты защиты и программное обеспечение в повседневной работе.

Предполагаемая продолжительность курса составляет 1 год. Рекомендуемый темп: 1 упражнение в неделю, выполнение каждого упражнения занимает от 5 до 45 минут.

## 3. Cybersecurity for IT Online (онлайн-курс по кибер- безопасности для ИТ-специалистов)

Интерактивный курс для всех ИТ-специалистов, который поможет освоить навыки реагирования на инциденты первого уровня.

Нельзя организовать надежную защиту цифрового пространства без систематического обучения всех сотрудников, которые в нем работают. Многие компании организуют обучение кибербезопасности на двух уровнях: экспертном (для специалистов) и базовом (повышение осведомленности обычных сотрудников). Однако ни один из этих уровней не подходит для большинства ИТ-специалистов, которые не занимаются непосредственно информационной безопасностью, но могут внести в нее конкретный и значимый вклад.

### Первая линия киберобороны

«Лаборатория Касперского» выпустила онлайн-курс для штатных ИТ-специалистов общего направления.

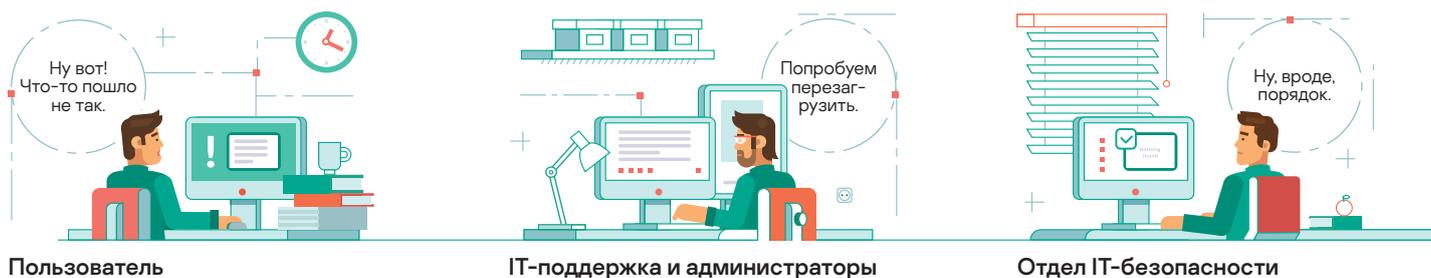
Курс состоит из 4 модулей:

- Вредоносное программное обеспечение
- Потенциально нежелательные программы и файлы
- Основы расследования инцидентов безопасности
- Реагирование на фишинговые атаки

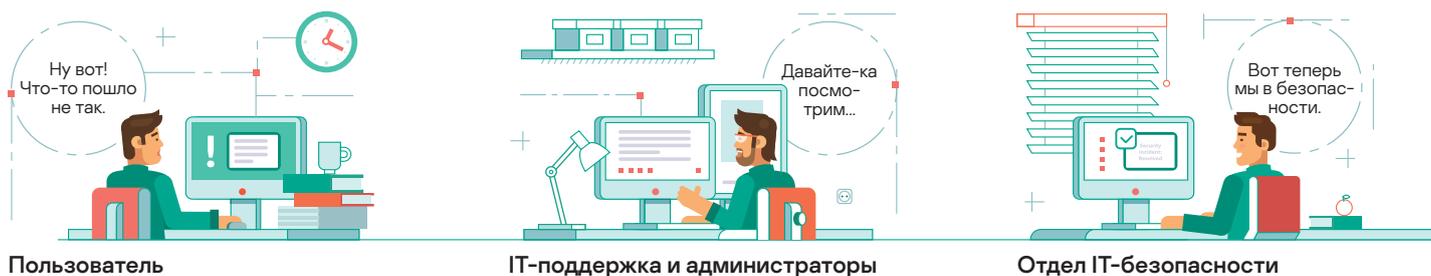
### Этот курс дает ИТ-специалистам следующие практические навыки

- Распознавание возможной атаки при изучении безобидного на первый взгляд инцидента безопасности на компьютере
- Сбор данных об инциденте для передачи в отдел ИТ-безопасности
- Поиск признаков кибератаки – это помогает всем ИТ-специалистам понять, что они должны делать на первой линии киберобороны.

#### Как обстоит дело сейчас



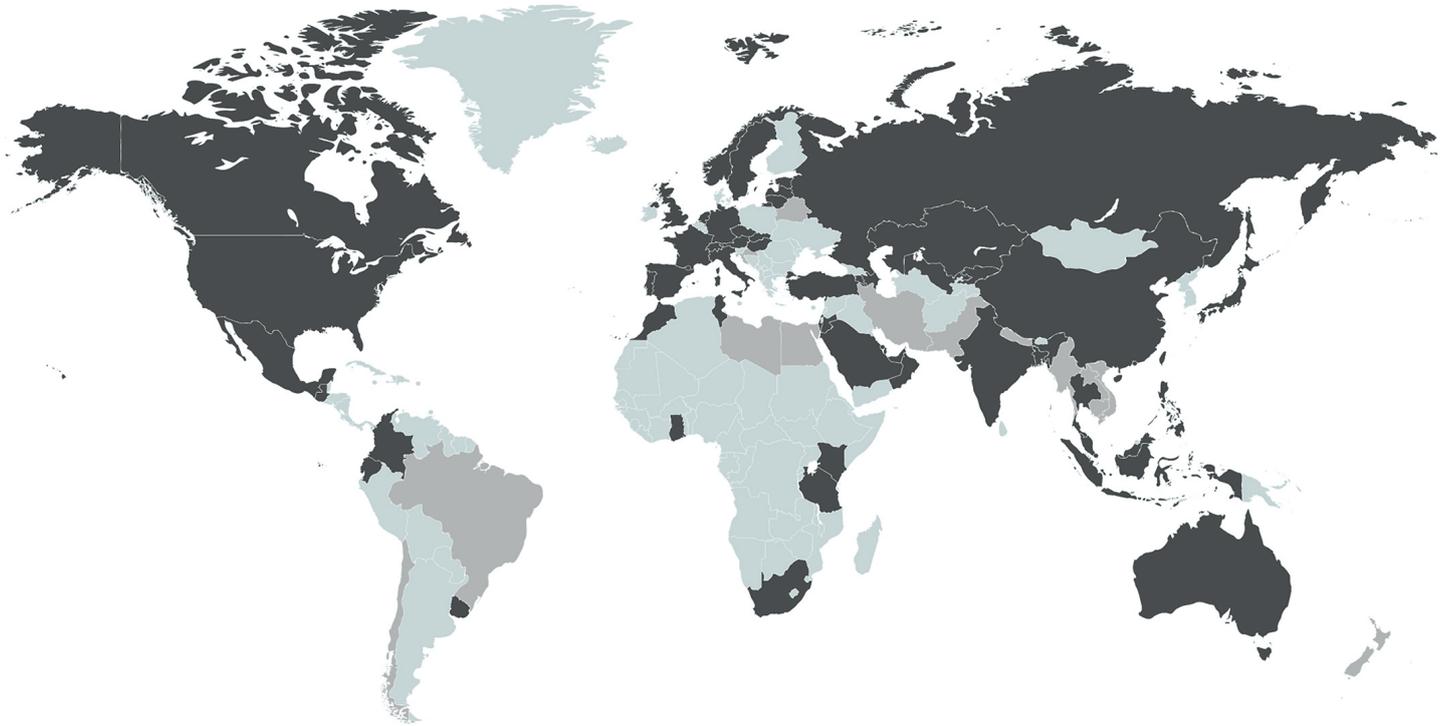
#### Как должно быть



**75**  
стран

**550 000**  
тысяч сотрудников

# Программы Kaspersky Security Awareness проходят по всему миру



По данным на март 2019 г.

- Использование в коммерческих целях или крупное мероприятие
- Участие в онлайн-турнире

Создано с помощью  
mapchart.net

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

© АО «Лаборатория Касперского», 2020.  
Все права защищены. Зарегистрированные товарные  
знаки и знаки обслуживания являются собственностью  
соответствующих владельцев.