



---

**Программы  
повышения  
осведомленности  
Kaspersky  
Security  
Awareness**

# **Kaspersky Gamified Assessment Tool**

**kaspersky**

# Оценка навыков кибербезопасного поведения

**Kaspersky Gamified Assessment Tool – это быстрый и увлекательный способ оценить навыки сотрудников в области кибербезопасности.**

**52%** крупных компаний и 50% предприятий малого и среднего бизнеса сталкивались с инцидентами кибербезопасности из-за неправильного использования IT-ресурсов сотрудниками\*

**42%** организаций отмечают, что неосведомленность сотрудников – это самая большая угроза кибербезопасности (неправильное использование IT-ресурсов, потеря корпоративных устройств, переход по фишинговым ссылкам и неумение распознать атаку с использованием социальной инженерии)\*

Почти **1 200 000 долларов США** составляет средний финансовый ущерб от утечек данных, вызванных неправильным использованием IT-ресурсов сотрудниками\*

**Во всем мире компании вкладывают немало сил и средств в создание все более сложных и эффективных систем защиты от киберугроз. И все же в информационной безопасности каждой организации остается то самое слабое звено, которое невозможно устранить техническими средствами.**

Речь о человеческом факторе. Именно он – одна из главных причин киберинцидентов. Изменить поведение сотрудников непросто. Людям неинтересно изучать кибербезопасность с помощью традиционных обучающих курсов: у них нет мотивации и зачастую они даже не подозревают, что имеют пробелы в знаниях. Как заинтересовать их? И как оценить уровень их знаний в сфере кибербезопасности? Мы предлагаем воспользоваться Kaspersky Gamified Assessment Tool – инструментом, который позволит быстро оценить текущие знания сотрудников и мотивировать их на развитие новых навыков. Короткая игра поможет IT- и HR-отделам получить полное представление об осведомленности сотрудников в вопросах кибербезопасности и будет первым этапом более развернутой программы тренингов.



## Что предлагает Kaspersky Gamified Assessment Tool?

- В нем есть три сценария оценки на основе знакомых ситуаций, требующих определенных навыков кибербезопасности: работа в офисе, в пути и дома.
- Каждому сотруднику предстоит решить 12 случайных задач в рамках сценария. Все они требуют знаний в области кибербезопасности. Необходимо проанализировать каждую ситуацию, оценить рискованность действий персонажа и указать степень своей уверенности в ответе с помощью фишек. За каждый ответ участнику начисляются баллы. При подсчете общего количества баллов система учитывает как сам ответ (верный или неверный), так и степень уверенности.
- Система выбирает сценарии случайным образом – это предотвращает читерство и делает процесс оценки увлекательным. Библиотека насчитывает 225 ситуаций, 12 из которых выбираются случайно для каждого сценария. Таким образом, всем участникам достаются разные задачи.
- Выполнив все задания, сотрудник получает оценку своих знаний и обратную связь с объяснениями и полезными советами.
- По окончании игры сотрудник получает сертификат, который можно скачать и показать другим пользователям.
- Администратор игры получает отчет с подробными результатами всех участников по каждой теме – с количеством баллов и правильных ответов, а также степенью уверенности в ответах. Такая развернутая оценка знаний сотрудников позволит эффективнее спланировать и организовать тренинг по кибербезопасности.

\* Отчет «Лаборатории Касперского» IT security economics in 2019 («Экономика IT-безопасности за 2019 год»)

# Kaspersky Gamified Assessment Tool оценивает знания сотрудников по следующим темам:

- Пароли и учетные записи
- Электронная почта
- Работа в интернете
- Социальные сети и мессенджеры
- Безопасность компьютеров
- Мобильные устройства

## Учебный процесс

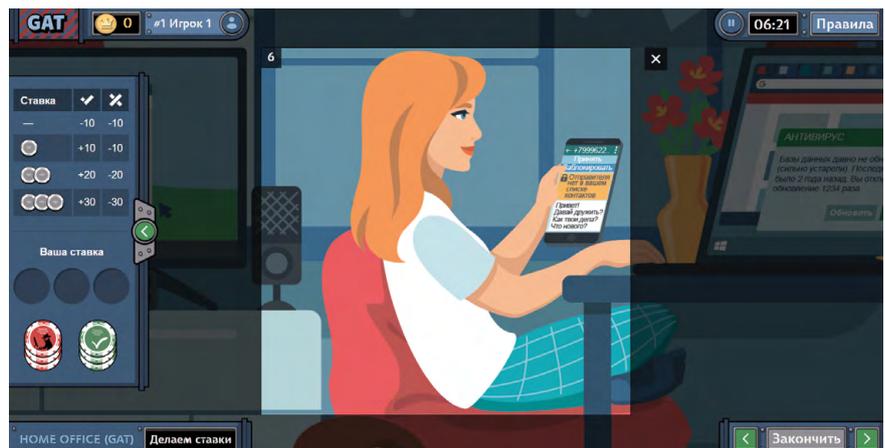
В начале игры система предлагает пользователям ознакомиться с правилами.



В течение 10 минут сотрудники должны проанализировать поведение персонажей в 12 ситуациях, связанных с кибербезопасностью, в рамках того или иного сценария. Им нужно решить, являются ли действия персонажа рискованными, указав в ответе степень своей уверенности. Игру можно приостановить. Если сотруднику нужно отвлечься, он может нажать паузу (кнопка в правом верхнем углу рядом с таймером).



Пользователи ставят **зеленые фишки**, если считают, что действия персонажа безопасны, и **красные**, если есть риск. Количество фишек указывает на степень уверенности в ответе.





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

## Ключевые особенности



### Глубокие знания в области кибербезопасности

Более 20 лет опыта в сфере IT-безопасности легли в основу наших курсов.



### Навыки, которые меняют поведение сотрудников на всех уровнях организации

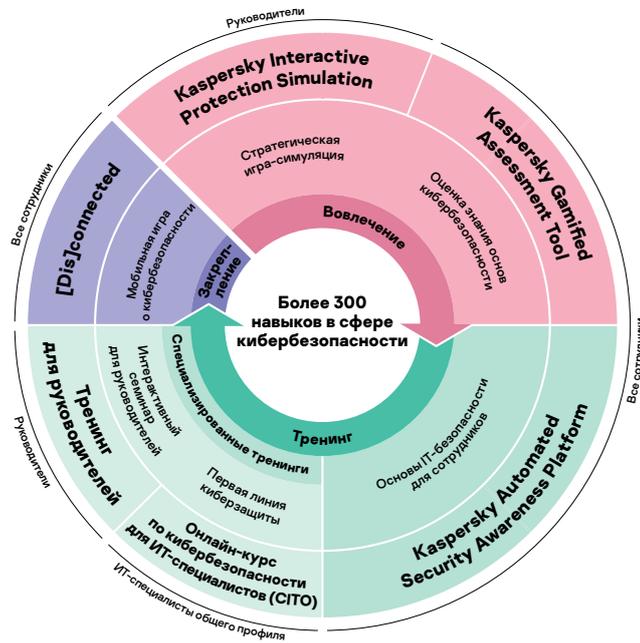
Игровой формат тренингов помогает заинтересовать и мотивировать сотрудников, а обучающие платформы позволяют закреплять полученные навыки.

Kaspersky Security Awareness предлагает ряд интересных и эффективных курсов для повышения осведомленности сотрудников и создания культуры кибербезопасности в организации. Поскольку для формирования устойчивых навыков безопасного поведения требуется время, наш подход подразумевает непрерывный и многокомпонентный цикл.

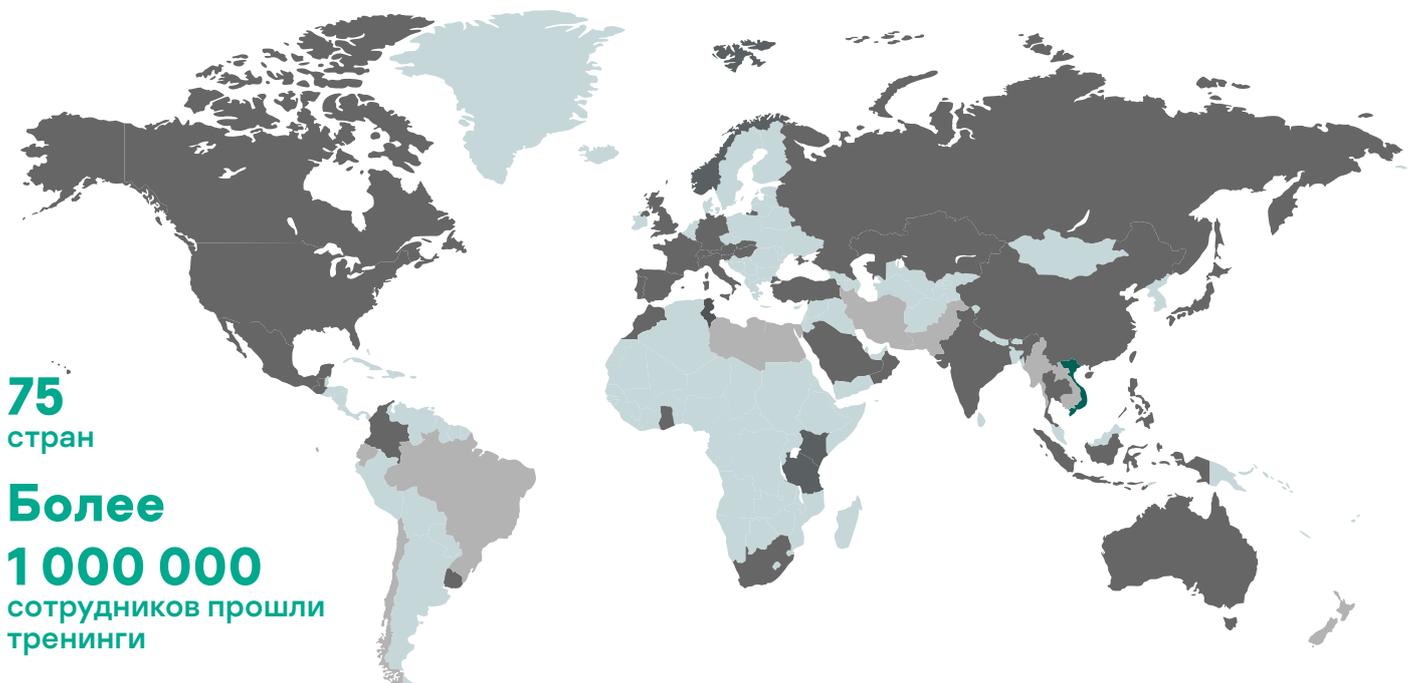
## Разные форматы тренингов для разных уровней организации

Выберите один тренинг для решения конкретной задачи безопасности или приобретите пакет тренингов, который можно адаптировать под ваши потребности и приоритеты.

Подробная информация о пакетах тренингов на сайте: [kaspersky.ru/awareness](https://kaspersky.ru/awareness)



## Тренинги Kaspersky Security Awareness проходят по всему миру



75  
стран

Более  
1 000 000  
сотрудников прошли  
тренинги

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

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

**kaspersky** АКТИВИРУЙ  
БУДУЩЕЕ