Тренинги
по повышению
киберграмотности
Kaspersky Security
Awareness

Игровой инструмент оценки

kaspersky.ru

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky
Gamified Assessment
Tool

Игровой инструмент оценки

Игровой инструмент оценки 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 ИТ-ресурсов сотрудниками*

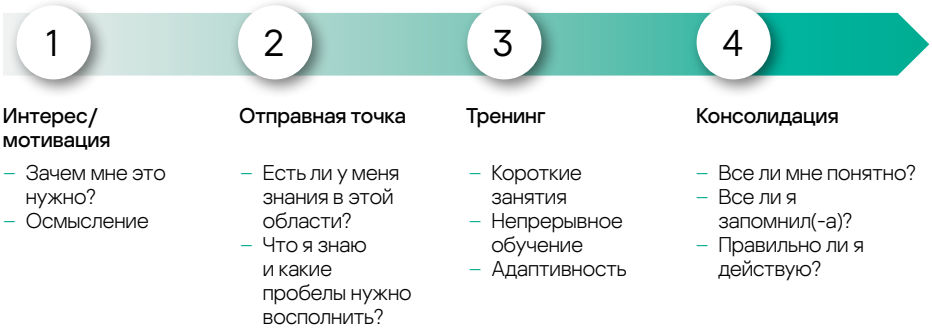
42% организаций отмечают, что неосведомленность сотрудников — это самая большая угроза кибербезопасности (ненадлежащее использование ИТ-ресурсов, потеря корпоративных устройств, переход по фишинговым ссылкам и неумение распознать атаки с использованием социальной инженерии)*

1195 тыс. долларов США составляет средний финансовый ущерб от утечек данных, вызванных ненадлежащим использованием ИТ-ресурсов сотрудниками*

Кибербезопасность — одна из главных сфер интересов современных предприятий. Тем не менее в ней остается много нерешенных задач. Во всем мире компании вкладывают немало сил и средств в разработку все более сложных и эффективных систем защиты от киберугроз. Тем не менее в структуре кибербезопасности каждой компании остается уязвимое место, которое невозможно устранить техническими средствами.

Это человеческий фактор. Человеческий фактор — одна из главных причин киберинцидентов. Изменить поведение сотрудников может оказаться непростым делом, поскольку они не заинтересованы в обучении кибербезопасности, у них низкая мотивация и зачастую они не осознают, что имеют пробелы в знаниях. Как повысить мотивацию сотрудников к обучению? Как оценить их текущий уровень знаний в сфере кибербезопасности? Игровой инструмент оценки позволяет быстро измерить текущий уровень навыков сотрудников в сфере кибербезопасности, а также мотивировать их к дальнейшему обучению. Небольшой игровой инструмент поможет руководителям ИТ-отдела или отдела кадров получить полное представление об осведомленности сотрудников в вопросах кибербезопасности и будет вводным этапом для дальнейшей программы по повышению киберграмотности сотрудников.

Непрерывный цикл обучения



Что включает игровой инструмент оценки?

- Существует три сценария, в которых нужно отработать определенные навыки кибербезопасности. Они соответствуют знакомым ситуациям: работа в офисе открытого типа, в командировке и из дома.
- Каждому сотруднику предстоит решить 12 случайных задач в рамках сценария. Все они требуют знаний 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.
- Библиотека насчитывает 225 ситуаций, 12 из которых выбираются случайно для каждого сценария. Таким образом, всем участникам достаются разные задачи, что предотвращает «списывание» и делает процесс оценки более увлекательным.
- После выполнения всех заданий сотрудник получает общую оценку своих знаний по кибербезопасности и обратную связь с объяснениями и полезными советами.
- По окончании процесса оценки выдается сертификат. Его можно скачать, распечатать и поделиться в соцсетях.
- Администратор игры получает отчет с подробными результатами всех участников по каждой теме: с количеством баллов и правильных ответов, а также степенью уверенности. Такая развернутая оценка знаний сотрудников позволит эффективнее спланировать и организовать тренинг по кибербезопасности.

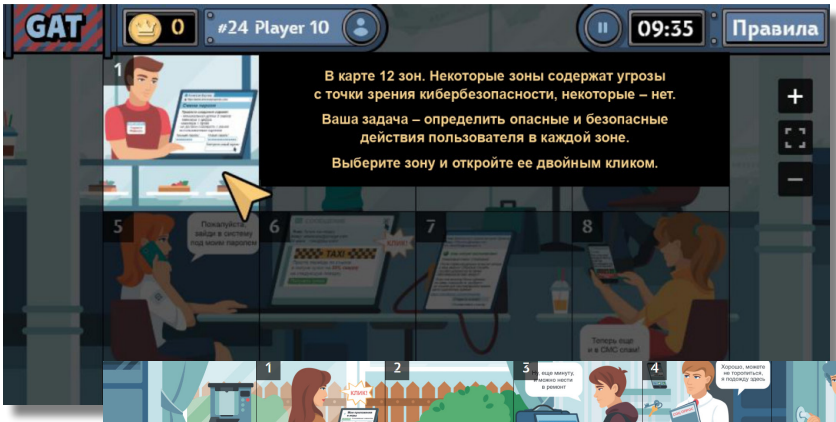
* По данным отчета «Экономика в ИТ-безопасности, 2019 год», «Лаборатория Касперского»

Игровой инструмент оценки охватывает знания сотрудников по следующим темам:

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

Процесс обучения

В начале игры пользователям предлагается ознакомиться с правилами.



В течение 10 минут сотрудники должны проанализировать поведение персонажей в 12 ситуациях, связанных с кибербезопасностью, в рамках того или иного сценария. Необходимо определить, 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).

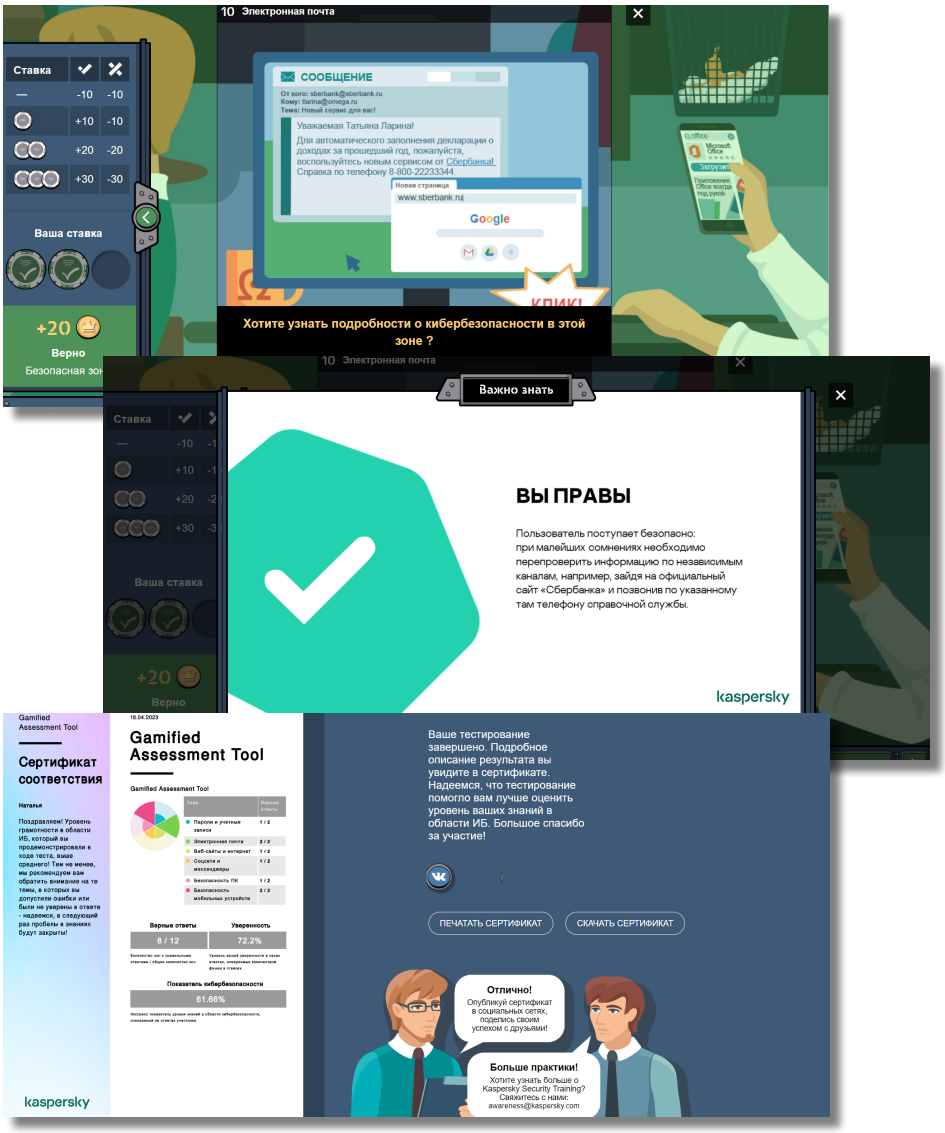
Пользователи ставят зеленые фишки, если считают действия персонажа безопасными, и красные, если есть риск. Количество фишек показывает степень уверенности в ответе.

Общее количество баллов в игре — это оценка уровня осведомленности сотрудника в сфере кибербезопасности.

Можно заново проанализировать каждую ситуацию.

И получить отзывы с пояснениями и рекомендациями по каждой ситуации.

По окончании игры участники получат сертификат с оценкой и рекомендациями по темам, на которые стоит обратить особое внимание во время предстоящего тренинга. Его можно скачать и поделиться.



Технические рекомендации

ОС:
Windows 7, 10;
Mac: Sierra, High Sierra, Mojave, Catalina;
Ubuntu 18.04.

Рекомендуем использовать следующие браузеры:
Firefox 70 или выше;
Chrome 80 или выше;
Safari 11 или выше.

Игровой инструмент оценки — это облачное решение, для использования которого на компьютере или планшете необходим только браузер с разрешением 1024x768 и выше.

Kaspersky Security Awareness — новый подход к совершенствованию навыков в области информационной безопасности

Ключевые особенности программы

Глубокие знания в области кибербезопасности
В результате более 25 лет работы на рынке решений кибербезопасности сформировался набор навыков, лежащий в основе 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.

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.

Бесплатная пробная версия платформы: k-asap.ru
Решения для защиты крупных предприятий: www.kaspersky.ru/enterprise
Kaspersky Security Awareness: www.kaspersky.ru/awareness
Новости ИТ-безопасности: business.kaspersky.ru

www.kaspersky.ru

kaspersky **АКТИВИРУЙ БУДУЩЕЕ**