Kaspersky Interactive Protection Simulation

Эффективный способ повысить осведомленность руководящих и принимающих решения сотрудников об угрозах кибер-безопасности

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Подробнее на сайте
kaspersky.ru/awareness

Kaspersky Interactive Protection Simulation

Проблема взаимопонимания

Сегодня одна из главных сложностей обеспечения безопасности на предприятиях состоит в том, что у разных руководителей различаются приоритеты, поскольку каждый смотрит на проблему по-своему. Это может привести к своеобразному «бермудскому треугольнику»:

- управляющие компанией могут считать обеспечение безопасности
- препятствием на пути к бизнес-целям (производить дешевле, быстрее или качественнее);
- ответственные за IT-безопасность часто думают, что такие аспекты, как распределение бюджета и налаживание инфраструктуры, находятся вне их компетенции;
- руководители, контролирующие расходы, не всегда понимают, как вложения в кибербезопасность связаны с прибылью и почему это не столько траты, сколько способ их избежать.

Взаимопонимание и партнерство этих трех сторон необходимы для эффективной защиты компании. Однако традиционные форматы повышения осведомленности, такие как лекции и учения с участием red team и blue team, – не лучший выбор. Они отнимают много времени, переполнены технической информацией и не подходят загруженным работой менеджерам. А главное – они не способствуют взаимопониманию по вопросам безопасности.

Кибербезопасность предприятия начинается с высшего руководства

Сегодня для многих компаний забота об устойчивости IT-инфраструктуры является приоритетом. Однако вопросы кибербезопасности обычно находятся в сфере ответственности IT- и ИБ-специалистов, что может приводить к фрагментации культуры безопасного поведения в масштабах всей организации. Руководители предприятий в первую очередь нацелены на рост продаж, повышение лояльности клиентов, сокращение рисков и издержек. При этом они часто упускают из виду вопросы кибербезопасности. Но если руководители личным примером не способствуют формированию единой культуры кибербезопасности на предприятии, эта цель может оказаться недостижимой.

76% руководителей компаний признались, что иногда обходят протоколы безопасности, чтобы быстрее выполнить какую-либо задачу, жертвуя безопасностью ради скорости*.

62% менеджеров признались, что недопонимание в вопросах информационной безопасности компании привело как минимум к одному киберинциденту**.

51% ИБ-сотрудников считают, что вопрос увеличения расходов на информационную безопасность очень сложно обсуждать. При этом все они владеют эффективными стратегиями коммуникации.

56% руководителей высшего звена и 48% IT-специалистов согласны с тем, что обсуждать вопросы информационной безопасности эффективнее всего на примерах реальных жизненных ситуаций**.

Как тренинги по кибербезопасности Kaspersky Security Awareness помогают в решении проблем

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.

Каждый продукт занимает определенное место в комплексном цикле обучения, при этом его можно приобрести и отдельно.

Стратегическая бизнес-игра для повышения киберграмотности руководителей компаний

Kaspersky Interactive Protection Simulation (KIPS) – это стратегическая бизнес-симуляция, командная игра, демонстрирующая, как кибербезопасность связана с эффективностью бизнеса.

Участники погружаются в симулированную бизнес-среду, где им в роли сотрудников ИБ-отдела предстоит столкнуться с множеством неожиданных киберугроз. Задача участников – постараться в этих условиях сохранить стабильную работу предприятия и уровень прибыли.

Им необходимо выстроить стратегию кибербезопасности, выбирая лучшие из доступных методов проактивной и реактивной защиты. Каждый выбор, который они совершают, определяет дальнейшее развитие сценария, а в конечном итоге – то, какую прибыль получит или не получит компания.

Сопоставляя приоритеты разработки, ведения бизнеса и безопасности с затратами в случае реалистичной кибератаки, команды анализируют данные и принимают стратегические решения в условиях нехватки достоверной информации и ограниченных ресурсов. Ситуации выглядят реалистично, поскольку в основе каждого сценария лежат события, произошедшие в реальности.

* https://www.forbes.com/sites/louiscolumbus/2020/05/29/cybersecuritys-greatest-insider-threat-is-in-the-c-suite/?sh=466624f87626

** https://www.kaspersky.com/blog/speak-fluent-infosec-2023/

KIPS – это динамичная игра, помогающая повысить знания о киберугрозах на практике.

- Интересный, увлекательный и динамичный тренинг (2 часа)
- Командная работа, формирующая атмосферу сотрудничества
- Элемент соревновательности, развивающий инициативность и аналитические навыки
- Игровая форма, позволяющая понять тактику и стратегию кибербезопасности
- Все сценарии и варианты атак основаны на реальных событиях

Почему KIPS эффективен?

Тренинг Kaspersky Interactive Protection Simulation предназначен для экспертов по бизнес-системам, IT-специалистов и линейных руководителей. Его цель – повысить знания участников о рисках и проблемах безопасности современных компьютерных систем.

Каждая команда из 4-6 человек получает задание руководить предприятием с производственными мощностями и управляющими производством компьютерами. В процессе игры предприятие должно генерировать прибыль, улучшать общественное мнение и бизнес-результаты. Одновременно команды должны бороться с кибератаками, угрожающими производительности предприятия.

По итогам тренинга участники приходят к важным практическим заключениям, которые смогут использовать в дальнейшей работе.

- Кибератаки бьют по прибыльности. Ими необходимо заниматься на самом высоком уровне.
- Сотрудничество между лицами, ответственными за принятие решений как в области IT, так и в других подразделениях, крайне важно для обеспечения эффективной киберзащиты любого предприятия.
- Разумные траты на киберзащиту не разорят предприятие, а потеря доходов в результате успешной кибератаки – может.
- Сотрудники быстро привыкают к мерам безопасности (аудитам, использованию антивирусного ПО и т. д.), понимая их необходимость.

Тренинг Kaspersky Interactive Protection Simulation можно проводить в двух форматах.

Очный формат **KIPS Live** очень популярен благодаря атмосфере воодушевления и энтузиазма, которая возникает во время тренинга. Это отличный инструмент для вовлечения сотрудников в формирование культуры кибербезопасности на предприятии.

В онлайн-формате **KIPS Online** пользователи могут взаимодействовать с большим количеством других участников, находясь в любом удобном месте.

Этот формат идеально подходит для международных организаций и массовых мероприятий. KIPS Online можно сочетать с форматом Live, чтобы в тренинге одновременно могли участвовать команды как в удаленном, так и в очном режиме.

- Одновременное участие до 300 команд (= 1000 участников), находящихся в любой точке мира
- Каждая команда может выбрать игровой интерфейс на нужном языке
- Клиенты могут персонализировать готовые сценарии, определяя количество атак в игре и выбирая различные виды атак из библиотеки.
- Клиенты, которые приобрели лицензию на неограниченное количество игр KIPS в период ее действия, могут играть с заранее заданными параметрами или персонализировать сценарий каждый раз, выбирая и комбинируя различные виды атак из библиотеки. Благодаря этой возможности условия игры каждый раз меняются, что делает ее еще интереснее.
- Еще одно преимущество онлайн-версии – возможность получать статистику о выборе игроков, данные о действиях команд в тех или иных ситуациях и сравнительный анализ поведения игроков по отношению к предыдущей игре.

KIPS помогает участникам понять:

- какова роль кибербезопасности в поддержании стабильной работы и доходности бизнеса;
- с какими проблемами и угрозами сталкиваются современные предприятия;
- какие типичные ошибки совершают компании, формируя стратегию кибербезопасности;
- как наладить сотрудничество между коммерческими отделами и службой безопасности, чтобы поддерживать стабильность операций и надежно защищать бизнес от киберугроз.

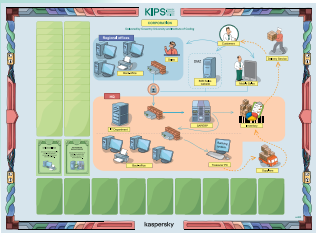
В рамках сценария команда участников отвечает за информационную безопасность предприятия в той или иной отрасли. Задача участников – обеспечить нормальную стабильную работу предприятия, сохранить отношения с клиентами с поставщиками, найти и нейтрализовать все источники киберугроз.

Когда компания подвергается кибератаке, команда видит последствия: снижение производительности и доходов компании. Чтобы преодолеть их и не потерять прибыль, приходится использовать различные бизнес- и IT-стратегии.

Побеждает команда, которая закончила игру с наибольшей прибылью, нашла и проанализировала все бреши в системе кибербезопасности, а также приняла все необходимые меры.

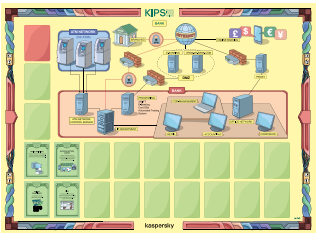
Корпоративные сценарии Kaspersky Interactive Protection Simulation для разных отраслей

Корпорация



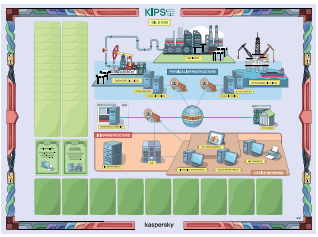
Защита предприятия от **программ-вымогателей, APT-угроз и уязвимостей систем автоматизации.**

Банк



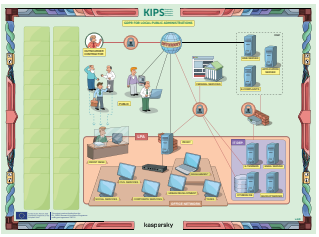
Защита финансовых организаций от **новейших высокоуровневых APT-угроз (Tyupkin, Carbanak и прочих).**

Нефтегазовая компания



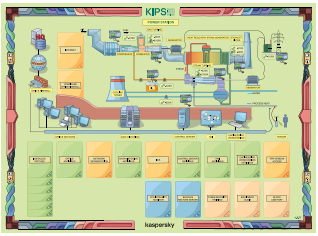
Анализ ущерба от различных кибератак, начиная с порчи **контента вебсайтов и заканчивая современными программами-вымогателями и изощренными APT-угрозами.**

Орган местного самоуправления



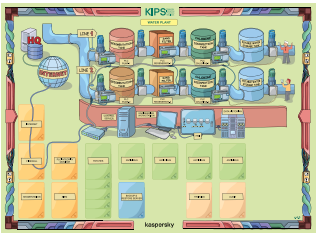
Защита веб-серверов государственных организаций от атак и эксплойтов.

Электростанция



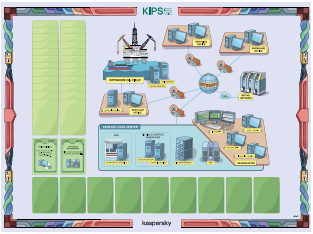
Защита промышленных систем управления и других критически важных компонентов инфраструктуры от киберугроз, аналогичных Stuxnet.

ГЭС



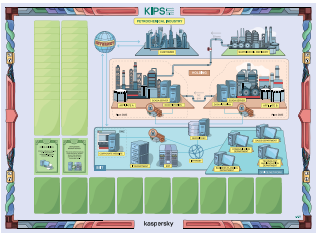
Защита IT-инфраструктуры предприятия по очистке воды для обеспечения стабильной работы двух производственных линий.

Нефтяной холдинг



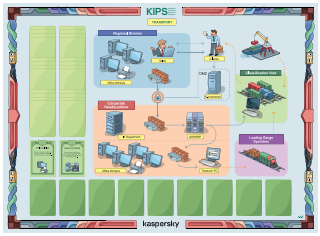
Обеспечение кибербезопасности для защиты прибыли транснациональной компании нефтяного и энергетического сектора с офисами по всему миру.

Нефтехимическое предприятие



Обеспечение бесперебойной работы нового филиала крупного нефтехимического холдинга, специализирующегося на производстве этилена.

Транспортные компании

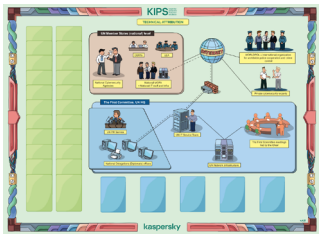


Защита транспортных компаний от **ошибок Heartbleed, APT-угроз, программ-вымогателей в корпоративном сегменте и инсайдерских атак.**

Аэропорт

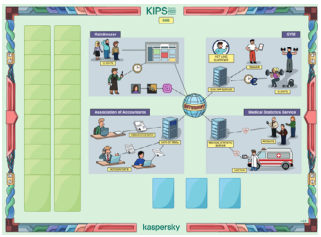
Защита активов аэропорта от многочисленных кибератак для обеспечения безопасности пассажиров и своевременной доставки грузов.

Атрибуция кибератак



Расследование и проведение атрибуции сложной APT-атаки на серверы ООН.

Малый и средний бизнес



Помощь предприятиям малого и среднего бизнеса в защите от таких киберугроз, как DDoS-атаки, программы-вымогатели, взлом мобильных приложений и кража личных данных.

Телекоммуникационные компании

Защита активов крупного телекоммуникационного холдинга, в который входят оператор связи, провайдер облачных услуг, разработчик игр и штаб-квартира.

Хотите получить еще больше пользы от KIPS?

Дополните опыт, полученный во время игры KIPS, тренингом **Executive Training**, также входящим в комплексный цикл Kaspersky Security Awareness. Этот тренинг для руководителей можно пройти до или после KIPS, в зависимости от вашего подхода к обучению. Закрепите опыт, полученный во время игры KIPS. Во время тренинга для руководителей вы узнаете, как современный ландшафт киберугроз может повлиять на ваш бизнес, поймете, как действовать в случае кибератаки, а также получите множество другой интересной, актуальной и полезной информации. Executive Training проводится в двух форматах: интерактивный офлайн-семинар или онлайн-курс.

Отзывы клиентов и пользователей о тренинге Kaspersky Interactive Protection Simulation

Тренинг Kaspersky Industrial Protection Simulation заставляет по-новому взглянуть на вещи. Он должен стать обязательным для всех специалистов по безопасности.

Уорвик Эшфорд (Warwick Ashford),
Computer Weekly

В ЦЕРН задействовано огромное количество IT- и инженерных систем, обслуживаемых тысячами людей. Поэтому с точки зрения кибербезопасности повышение осведомленности сотрудников и формирование у них навыков безопасного поведения имеют не меньшее значение, чем технические средства. Тренинг «Лаборатории Касперского» оказался интересным, занимательным и эффективным.

Стефан Лудерс (Stefan Luders),
директор по информационной безопасности, ЦЕРН

Мы посмотрели на кибербезопасность под новым углом. А некоторые участники спрашивали, нельзя ли использовать эту игру в их компаниях.

Джо Вайс (Joe Weiss),
инженер-эксперт, сертифицированный руководитель службы информационной безопасности, сертифицированный специалист по контролю рисков и информационных систем, член ISA

Нам нужно создать единую сеть сотрудников, основанную на взаимодействии, и тренинг «Лаборатории Касперского» – прекрасный способ начать эту работу.

Даниэл П. Багге (Daniel P. Bagge),
национальный центр кибербезопасности Чехии

Рекомендации по подготовке к тренингу

Время проведения. Тренинг можно запланировать отдельно, а можно – как занятие в рамках другого мероприятия, например конференции или семинара. В этом случае оптимальное время для проведения игры – вечер первого дня.

Группа. Тренинг рассчитан на 20–100 человек (по 3–4 участника в команде). В идеале в каждую команду должны входить сотрудники разных отделов (управленческого, инженерного, отдела информационной безопасности и т. д.).

- В команде должно быть хотя бы по одному представителю от каждого подразделения/должности.
- В команду могут входить люди как из одной, так и из разных компаний или отделов.
- Участники необязательно должны быть знакомы друг с другом.

Подготовка. Сама игра занимает от 1,5 до 2 часов, но доступ в помещение для команды ведущих из «Лаборатории Касперского» необходимо открыть за 2 часа до начала – для подготовительных работ.

Помещение. Следует выделить по 3 кв. м на человека; помещение должно быть без колонн. Требуется стандартное аудио- видео-оборудование: проектор (6–8 люменов), экран, аудиосистема (динамики, пульт дистанционного управления, микрофоны).

Также необходимы: сеть Wi-Fi с доступом в интернет со скоростью от 4 Мбит/с (для подключения к игровому серверу) и по одному планшету iPad (или другой марки) с поддержкой Wi-Fi на каждую команду из 4-х человек.

Мебель. Столы для участников на 4 человека (прямоугольные размером не менее 75 x 180 см или круглые диаметром не более 1,5 м). Участники рассаживаются за столами группами по 4 человека. Также необходимы столы для ведущих и стулья для всех участников.

Примеры успешного сотрудничества

Игровой тренинг KIPS прошли специалисты по промышленной безопасности более чем из 50 стран.

- KIPS был переведен на русский, английский, немецкий, французский, японский, испанский (для Евросоюза и для стран Латинской Америки), португальский, турецкий, итальянский, китайский, голландский и арабский языки.
- KIPS используется многими правительственными организациями, в том числе ведомством по кибербезопасности Малайзии, агентством национальной безопасности Чехии, национальным центром кибербезопасности Нидерландов, для повышения уровня знаний сотен экспертов, задействованных в защите критически важных государственных инфраструктур.
- KIPS лицензирован ведущими регуляторами в области обучения, такими как институт SANS. Этот тренинг проходят обучающиеся по программам кибербезопасности SANS во всем мире.
- KIPS лицензирован производителями и поставщиками решений безопасности, в том числе компанией Mitsubishi-Hitachi Power Systems, где он используется как тренинг для клиентов, обслуживающих критически важную инфраструктуру.
- KIPS является частью проекта GEIGER Европейской комиссии, направленного на киберзащиту малых и микропредприятий, обучение их сотрудников и улучшение управления персональными данными.

Подготовка инструкторов

Если клиент хочет использовать Kaspersky Interactive Protection Simulation для обучения большого количества сотрудников, руководителей и экспертов из разных отделов и филиалов, можно приобрести лицензию на проведение тренингов KIPS, подготовить инструкторов внутри компании и организовать обучение в удобном темпе и формате.

Эта лицензия включает:

- право использовать программу тренингов Kaspersky Interactive Protection Simulation внутри организации;
- набор материалов для тренинга, право использовать и воспроизводить их;
- логин и пароль для входа на сервер тренинга в период действия лицензии;
- руководство для инструктора, обучение и рекомендации для руководителей программы по организации и проведению тренингов KIPS;
- обслуживание и поддержку (обновление и поддержка программного обеспечения и содержимого тренингов);
- адаптацию сценариев игры к требованиям клиента (опционально, за дополнительную плату).

KIPS для партнеров и учебных центров

KIPS дает партнерам прекрасную возможность получать выгоду, используя это решение несколькими разными способами. Они могут продавать его как продукт, предлагать клиентам своих учебных центров и даже проводить тренинги самостоятельно. Если партнеры выбирают последний вариант, специалисты «Лаборатории Касперского» могут обучить их сотрудников навыкам, необходимым для проведения тренингов.

Kaspersky Security Awareness

Ключевые особенности программы

Глубокие знания в области кибербезопасности

За более чем 25 лет работы в области кибербезопасности мы сформировали набор навыков, который лег в основу наших продуктов.

Тренинги, которые меняют поведение сотрудников на всех уровнях организации

Игровой формат тренингов помогает заинтересовать и мотивировать сотрудников, а упражнения позволяют закреплять полученные навыки

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

Поскольку для формирования устойчивых навыков безопасного поведения требуется время, наш подход подразумевает непрерывный и многокомпонентный цикл обучения. 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.

Непрерывный цикл обучения

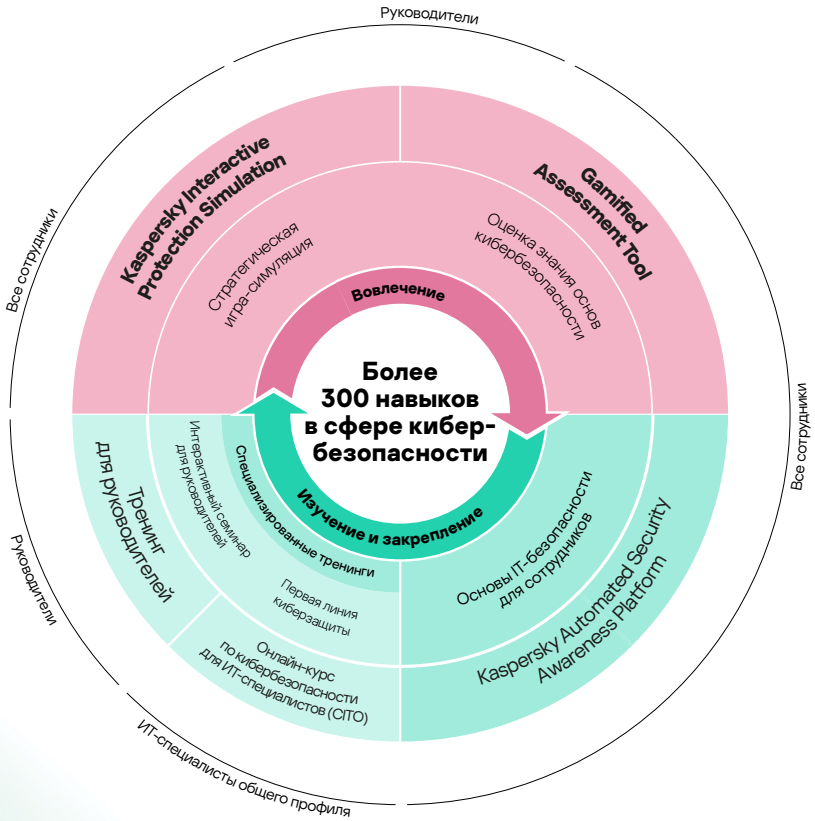
Интерес/ Мотивация
- Зачем мне это нужно?
- Осмысление

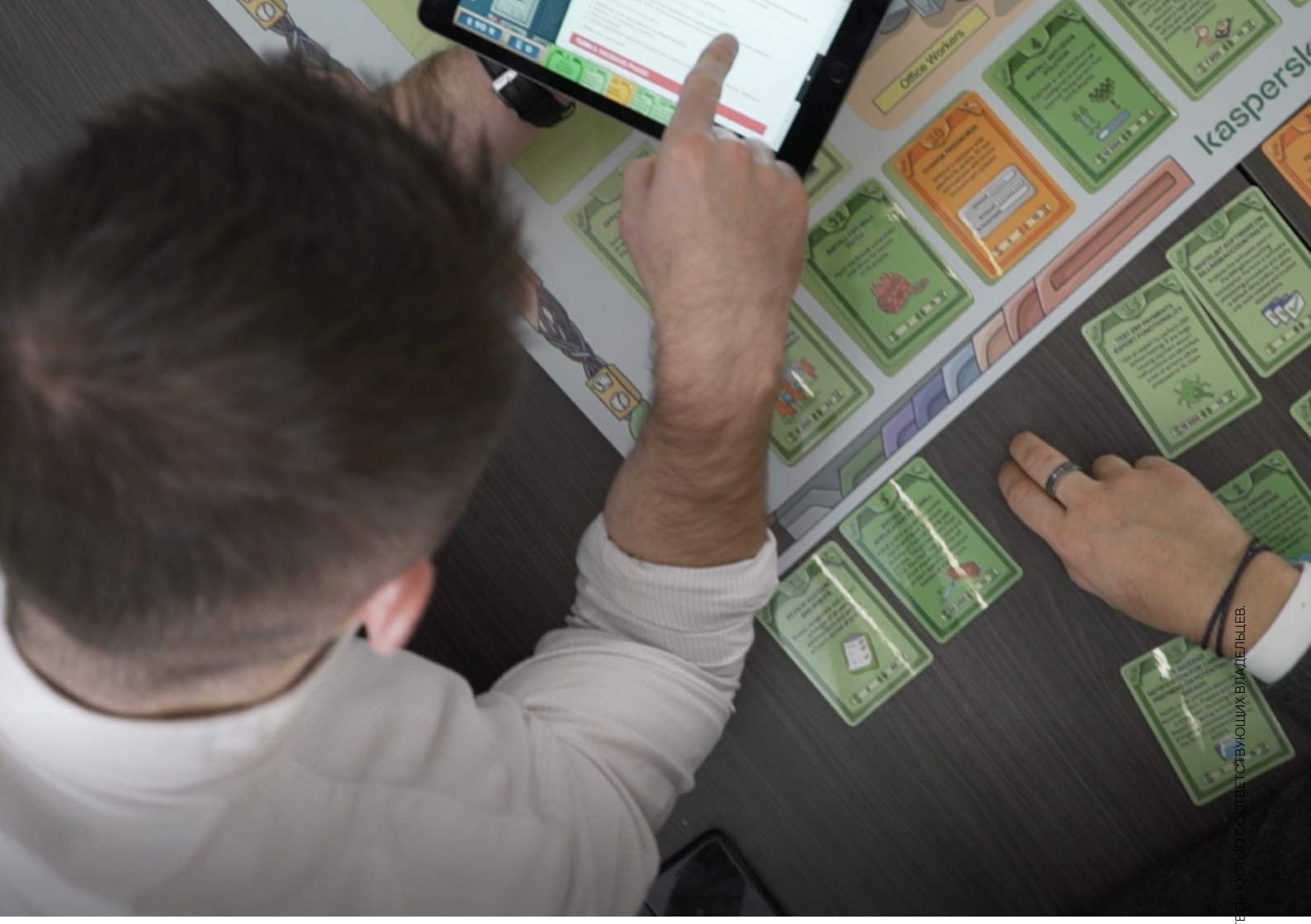
Отправная точка
- Есть ли у меня знания в этой области?
- Что я знаю, и какие пробелы нужно восполнить?

Тренинг
- Короткие занятия
- Непрерывное обучение
- Адаптивность

Закрепление
- Все ли мне понятно?
- Все ли я запомнил(-а)?
- Правильно ли я действую?

Разные форматы тренингов для разных уровней организации





Решения для защиты крупных предприятий:
www.kaspersky.ru/enterprise
Kaspersky Security Awareness:
www.kaspersky.ru/awareness

www.kaspersky.ru

kaspersky