Эффективный способ повысить осведомленность руководящих и принимающих решения сотрудников об угрозах кибербезопасности

Kaspersky Interactive Protection Simulation

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Подробнее на kaspersky.ru/awareness

Kaspersky Interactive Protection Simulation

Проблема взаимопонимания
Одна из главных сложностей обеспечения безопасности – 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 и 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 траты, а способ их избежать.

Взаимопонимание и партнерство этих трех сторон необходимы для эффективной защиты компании. Однако традиционные форматы повышения осведомленности, такие как лекции и обычная симуляция угроз для проверки реакции, – не лучший выбор. Они отнимают много времени, перенасыщены технической информацией и не подходят загруженным работой менеджерам. А главное – они не способствуют взаимопониманию по вопросам безопасности.

Что такое Kaspersky Interactive Protection Simulation?

Kaspersky Interactive Protection Simulation (KIPS) – это интерактивный тренинг, погружающий руководителей и других специалистов организаций в симулированную бизнес-среду, где им предстоит столкнуться со множеством неожиданных киберугроз. Задача участников – постараться в этих условиях максимально повысить прибыль и сохранить доверие к своей игровой компании.

Идея KIPS состоит в том, чтобы выстроить стратегию кибербезопасности, выбирая лучшие методы проактивной и реактивной защиты. Каждое действие команды-участника в ответ на происходящие события определяет дальнейшее развитие сценария, а в конечном итоге – то, какую прибыль получит или не получит «предприятие».

Сопоставляя приоритеты разработки, ведения бизнеса и безопасности с затратами в случае реалистичной кибератаки, команды анализируют данные и принимают стратегические решения в условиях нехватки информации и ограниченных ресурсов. Таким образом создается приближенная к жизни ситуация: в основе каждого сценария лежат события, произошедшие в реальности.

Почему KIPS эффективен?

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

Для защиты бизнеса участники должны принимать стратегические, управленческие и технические решения, учитывая эксплуатационные ограничения и поддерживая высокую прибыль.

Kaspersky Interactive Protection Simulation – это динамичная игра, помогающая повышать осведомленность 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.

Участники тренинга приходят к следующим важным заключениям, которые помогают им в реальной жизни:

- Кибератаки бьют по прибыльности. Ими необходимо заниматься на самом высоком уровне.
- Сотрудничество между IT- и бизнес-отделами необходимо для эффективной защиты предприятия.
- Бюджет на обеспечение безопасности – гораздо меньше прибыли, которую рискует потерять компания.
- Сотрудники привыкают к определенным мерам безопасности, понимая их важность и необходимость.

Тренинг помогает участникам понять:

- Какова роль кибербезопасности для поддержания 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 защищать бизнес от киберугроз.

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

Каждый сценарий построен вокруг определенного вектора угроз. Это позволяет выявлять и анализировать типичные ошибки, возникающие в той или иной отрасли при создании стратегий защиты и реагирования на инциденты.

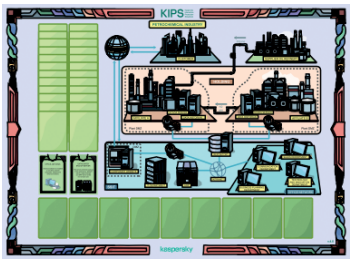
Так, в 2019 году появился новый сценарий, направленный на защиту персональных данных в органах местного самоуправления. В комплексе с другими упражнениями и учебными модулями тренинг повышает осведомленность служащих о киберугрозах и помогает выстроить позитивную модель поведения. Он акцентирует внимание участников на том, как важно работать сообща и грамотно распределять полномочия, чтобы принимать верные решения в вопросах безопасности граждан.

Также в конце 2019 года появилось 2 новых индустриальных сценария: «Нефтехимическое предприятие» и «Аэропорт».

В рамках сценария каждая команда отвечает за IT-безопасность в новом филиале крупного нефтехимического холдинга. Так как в филиале еще не внедрили все меры безопасности, принятые в компании, он становится слабым звеном с точки зрения защиты. Задача участников – обеспечить нормальную работу филиала, сохранить важных клиентов и хорошие отношения с поставщиками, найти и нейтрализовать все источники киберугроз.

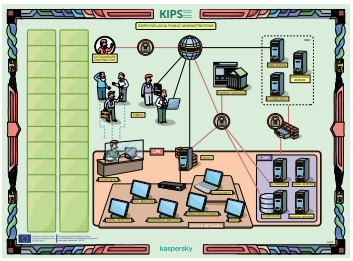
Сценарии Kaspersky Interactive Protection Simulation для разных предприятий

Нефтехимическое предприятие НОВИНКА!



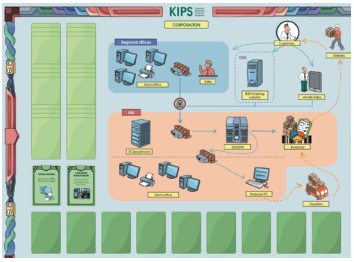
Поддержка бизнес-операций нового филиала крупного нефтехимического холдинга, специализирующегося на производстве этилена.

Орган местного самоуправления



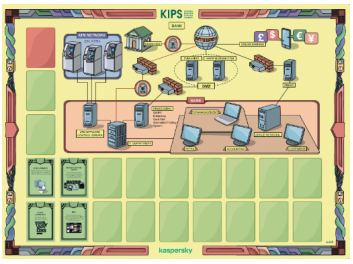
Защита веб-серверов государственных организаций от атак и эксплойтов.

Корпорация



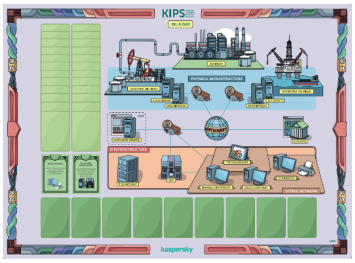
Защита крупного предприятия от **программ-вымогателей, APT-угроз и уязвимостей систем автоматизации.**

Банк



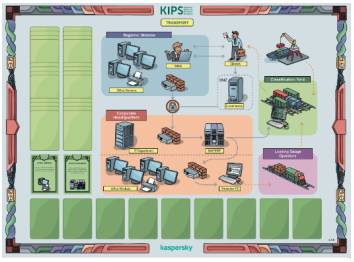
Защита финансовых организаций от **новейших высокоуровневых APT-угроз (Tyupkin, Carbanak и прочих).**

Нефтегазовая компания



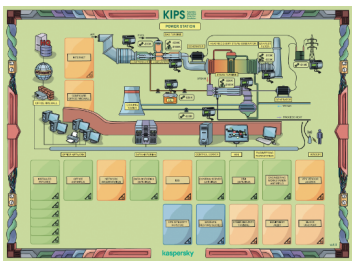
Анализ ущерба от различных кибератак, начиная **порчей контента веб-сайтов и заканчивая современными программами-вымогателями и изощренными APT-угрозами.**

Транспортная компания



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

ГЭС или электростанция



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

Аэропорт НОВИНКА!

Безопасность аэропорта с точки зрения ИТ: **безопасность пассажиров в аэропорту, грузов и полетов.**

Отзывы о тренинге Kaspersky Interactive Protection Simulation
Интерактивный тренинг «Лаборатории Касперского» по защите промышленных систем 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 безопасности повышение осведомленности и вовлечение сотрудников в выполнение защитных мер имеют такое же значение, как и технические средства. Тренинг «Лаборатории Касперского» оказался интересным, занимательным и эффективным.

Стефан Лудерс (Stefan Luders),
руководитель 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 м2 на человека; помещение должно быть без колонн, правильной формы. Требуется проектор (6–8 люменов), экран, аудиосистема (динамики, пульт дистанционного управления, микрофоны).

Также необходимы сеть **Wi-Fi** с доступом в интернет (для подключения к игровому серверу), скорость от 4 Мбит/с, по 1 планшету iPad (или другой марки) накаждую команду (4 человека) с поддержкой Wi-Fi.

Мебель. Понадобятся столы, рассчитанные на 4 человек (прямоугольные, размером не менее 75x180 см или круглые диаметром не более 1,5 м). Участники рассаживаются за ними группами по 4 человека. Также необходимы столы для ведущих и стулья по числу участников за столами.

Примеры из практики и отзывы

Тренинг «Лаборатории Касперского» прошли специалисты по промышленной безопасности более чем из 50 стран.

Игра использовалась правительственными организациями, такими как:

- Ведомство по кибербезопасности Малайзии, агентство национальной безопасности Чехии и национальный центр кибербезопасности Нидерландов, многими другими крупными государственными учреждениями.
- Kaspersky Interactive Protection Simulation использовался такими компаниями, как BASF (крупнейший в мире производитель химической продукции), ЦЕРН (чей главный проект – Большой адронный коллайдер), Mitsubishi, Yokogawa, «РусГидро», Panasonic, а также Международной ассоциацией автоматизации (ISA) для обучения сотрудников: инженеров, разработчиков и специалистов по работе с клиентами. Игра формирует представление о кибербезопасности в автоматизированных промышленных средах и учит соблюдению защитных мер.
- Тренинг лицензирован ведущими регуляторами в области обучения, такими как институт SANS; его проходят обучающиеся по программам кибербезопасности SANS во всем мире.
- Тренинг лицензирован производителями и поставщиками решений для безопасности, включая компанию Mitsubishi Hitachi Power Systems, для использования в качестве обучающего курса для пользователей, обслуживающих критически важную инфраструктуру.

Две формы проведения тренинга

Kaspersky Interactive Protection Simulation Live

Этот формат имеет больше ограничений, но способствует активному вовлечению в процесс, ведь непосредственная близость с другими участниками повышает интерес команд. В таком виде тренинг хорошо подходит для тимбилдинга.

- До 80 участников в одном помещении.
- Один язык проведения для всех участников.
- Присутствие инструктора и ассистента.
- Необходимы раздаточные материалы.

Kaspersky Interactive Protection Simulation Online

Этот вариант идеально подходит для международных организаций и массовых мероприятий. Его можно сочетать с форматом Live, чтобы в тренинге можно было участвовать очно и в удаленном режиме.

- Одновременное участие до 300 команд (= 1000 участников), находящихся в любой точке мира.
- Каждая команда может выбрать игровой интерфейс на нужном языке.
- Преподаватель ведет занятие через WebEx.

Подготовка инструкторов

Если клиент хочет использовать тренинг для обучения большого количества сотрудников, руководителей и экспертов из разных отделов и филиалов, можно приобрести лицензию на проведение тренингов, обучить инструкторов внутри организации и организовать обучение в удобном формате.

Лицензию можно получить у «Лаборатории Касперского». Она включает:

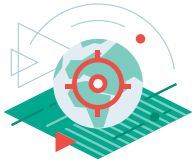
- Право использовать Kaspersky Interactive Protection Simulation внутри организации
- Набор материалов, право использовать и воспроизводить их
- Имя пользователя и пароль для входа на сервер тренинга
- Руководство для инструктора, обучение и рекомендации для руководителей программы по проведению тренингов
- Обслуживание и поддержка (обновления и поддержка программного обеспечения и обучающего контента)
- Адаптация сценария игры к требованиям клиента (доступна за отдельную плату)

Kaspersky Security Awareness

«Лаборатория Касперского» предлагает тренинги по повышению осведомленности в сфере кибербезопасности, в которых применяются лучшие образовательные методики и технологии.

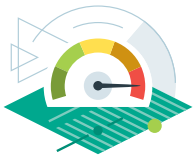
Этот подход меняет поведение пользователей и помогает создать безопасную информационную среду во всей организации.

Ключевые особенности программы



Только нужные навыки и знания
Цели для сотрудника соответствует его роли в компании и профилю рисков.
- Приводятся примеры из реальной жизни и развиваются навыки, которые можно сразу же применить.
- Сотрудники учатся на практике.

Человеко-ориентированный подход
Тренинг ориентирован на естественный способ мышления.
- Правила безопасности объясняются в проактивном и позитивном ключе.
- Сотрудники получают сведения и навыки, которые легко усвоить и закрепить благодаря методикам, учитывающим особенности человеческой памяти.



Постепенное повышение уровня сложности
- Принцип «от простого к сложному».
- Применение и расширение полученных ранее знаний в новых ситуациях.

Простота управления и контроля
- Онлайн-формат.
- Автоматическое управление.
- Каждому участники тренинга по электронной почте автоматически отправляются приглашения и мотивационные письма с индивидуальными рекомендациями.

Разные форматы обучения для разных уровней организации

Обучающие продукты **Kaspersky Security Awareness** состоят из трех связанных компонентов, которые можно эффективно использовать вместе и по отдельности.

Решения для крупного бизнеса: www.kaspersky.ru/enterprise
Kaspersky Security Awareness: www.kaspersky.ru/awareness

www.kaspersky.ru

kaspersky