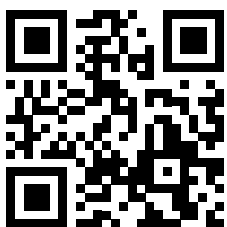

Эффективно
для сотрудников.
Просто для
руководителей.

k-asap.ru



Kaspersky Automated Security Awareness Platform

kaspersky АКТИВИРУЙ
БУДУЩЕЕ



Kaspersky
Automated Security
Awareness Platform

Kaspersky Automated Security Awareness Platform

Более 80% всех инцидентов кибербезопасности связаны с человеческим фактором. Из-за каждого такого инцидента компания может понести миллионные убытки. Однако традиционные тренинги, которые должны предотвращать проблемы, недостаточно эффективны, поскольку не всегда могут сформировать у сотрудников правильное поведение.

Человеческий фактор как основной киберриск сегодня

1 315 000 долл. США
на крупную компанию

составляет средний финансовый ущерб от утечек данных, вызванных неправильным использованием ИТ-ресурсов сотрудниками*

132 000 долл. США
на предприятие сегмента малого и среднего бизнеса

составляет средний финансовый ущерб от утечек данных, вызванных неправильным использованием ИТ-ресурсов сотрудниками*

50%
компаний

сообщили об угрозах, возникших в результате ненадлежащего поведения сотрудников. Это подтверждает, что человеческий фактор – самая распространенная угроза ИТ-безопасности*

43%
сотрудников

компаний малого бизнеса пострадали от инцидентов безопасности, произошедших из-за нарушения сотрудниками политик ИТ-безопасности*

26%
организаций

сотрудников сообщили, что их пароли от личной электронной почты и рабочей учетной записи совпадают**

Преграды на пути к внедрению эффективной программы повышения осведомленности о киберугрозах

Компании по всему миру внедряют программы повышения осведомленности о киберугрозах, но зачастую процесс обучения сотрудников и его результаты оставляют желать лучшего. Чаще всего со сложностями сталкиваются предприятия малого и среднего бизнеса: как правило, им не хватает опыта и ресурсов.

Неэффективный тренинг



Тренинг воспринимается как трудная, скучная, неактуальная обязанность



Упор делается на запреты, а не на примеры того, как нужно поступать



Знания не закрепляются



Читать и слушать объяснения – не так эффективно, как участвовать в практических занятиях

Дополнительная административная нагрузка



Как разработать программу и определить цели?



Как управлять заданиями в рамках тренинга?



Как контролировать продвижение по программе?



Как заинтересовать сотрудников в тренинге?

* По данным отчета «Экономика в ИТ-безопасности, 2021 год», «Лаборатория Касперского»

** <https://www.beyondidentity.com/blog/password-sharing-work>

Эффективные тренинги и простое управление для организаций любого масштаба

Представляем автоматизированную платформу для повышения осведомленности о кибербезопасности – ключевой компонент программы тренингов Kaspersky Security Awareness.

Платформа представляет собой онлайн-инструмент, помогающий постепенно выработать у сотрудников эффективные и практические навыки кибергигиены. Запуск и использование платформы не требуют специальных ресурсов и подготовки. На каждом этапе создания безопасной корпоративной киберсреды вам помогают встроенные подсказки.

Как оценить программу повышения осведомленности

Один из важнейших критериев оценки программы повышения осведомленности о кибербезопасности – ее эффективность. В случае Kaspersky Automated Security Awareness Platform эффективность является неотъемлемой характеристикой как самого тренинга, так и системы управления платформой. Контент платформы базируется на модели компетенций, включающей 350 практических и критически важных навыков кибербезопасности, которыми должны обладать все сотрудники. Без этих навыков сотрудники по незнанию или халатности могут нанести ущерб вашему бизнесу.

Эффективные тренинги

Систематизированное содержание	Тщательно продуманный и структурированный контент: – Интерактивные уроки, постоянное закрепление материала и имитации фишинговых атак, которые помогают применять на практике полученные знания Материалы тренингов и их структура организованы с учетом способности усваивать и сохранять информацию и других особенностей человеческой памяти.
Практический подход и вовлеченность	– Прямое отношение к повседневной работе участников – Навыки, которые можно немедленно применить Примеры реальных ситуаций, в которых сотрудники могут узнать себя, повышают вовлеченность участников в процесс прохождения тренинга и помогают запоминать информацию.
Позитивный настрой	Объяснение правил безопасности идет проактивно. В процессе тренинга вместо насаждения запретов даются ответы на вопросы «зачем» и «как». Переизбыток правил и ограничений вызывает отторжение, в то время как разъяснения и убеждения, которые выстроены с учетом особенностей человеческого мышления, помогают принять новую модель поведения.

Простое управление

Простое управление	Полностью автоматизированное управление позволяет каждому сотруднику овладеть навыками кибербезопасности в соответствии с его профилем рисков без вмешательства администратора платформы.
Простой контроль	Единая панель и актуальные отчеты.
Простое вовлечение	Платформа автоматически рассылает приглашения и мотивирующие письма в дополнение к еженедельным отчетам для обучающихся и администраторов.

Запуск программы в 4 шага

Загрузите
информацию
о пользователях

Сгруппируйте
пользователей по
профилям рисков
и задайте целевые уровни
для каждой группы

Запустите
тренинг

Автоматизиро-
ванное управле-
ние тренингом
осуществляется
платформой

Это единственный шаг, на котором администратору нужно будет анализировать и принимать решения.

Платформа составляет план прохождения тренинга для каждой группы в соответствии с темпом прохождения целевыми уровнями, предоставляет отчеты с рекомендациями.

Лучшие методики

Платформа Kaspersky ASAP предлагает новый способ предоставления учебных материалов по кибербезопасности. Можно либо назначить сотрудникам экспресс-курс, который поможет быстро освоить базовый набор навыков кибербезопасного поведения или освежить знания, либо выбрать полный курс, разбитый на уровни сложности.

Экспресс-курс

Краткая версия тренинга в аудио и видео формате. Каждый из 6 основных разделов курса содержит несколько коротких уроков, направленных на освоение базовых навыков кибербезопасности.

- Интерактивная теоретическая часть
- Видео-уроки
- Тестирование

Имитация фишинговых атак не входит в курс тренинга, но может быть назначена администратором дополнительно в рамках антифишинговой кампании.

Специализированные курсы для разных профилей рисков

Сотрудники автоматически распределяются по группам в соответствии с целевым уровнем знаний. Целевой уровень зависит от рисков, связанных с той или иной должностью. Чем выше риски, тем глубже должны быть знания. Так, работа IT-специалистов и бухгалтеров сопряжена с более высокими рисками по сравнению с основной массой сотрудников.

Гибкость

- В платформе реализован гибкий подход к тренингу, процессом последовательно и автоматизированно управляет сама платформа.
- Для каждой группы сотрудников можно выбрать:
 - темы, которые учащимся в этой группе предстоит освоить (темы, которые пока не нужны, можно пропустить);
 - целевой уровень, которого должны достичь учащиеся при изучении той или иной темы.
- Сотрудники не будут тратить время на изучение тем, не имеющих отношения к их работе.

Подробные актуальные отчеты в любое время

- На информационных панелях представлены все необходимые сведения.
- Платформа рекомендует, что нужно сделать, чтобы улучшить результаты.
- Отчеты загружаются с главной страницы одним щелчком мыши; можно настроить частоту получения отчетов по электронной почте.

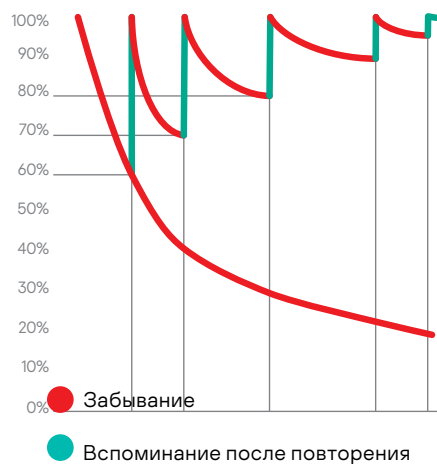
Гибкий учебный план

Методы получения знаний: основной курс

Постепенное повышение уровня сложности

Кривая Эббингауза (кривая забывания)

Многочратное повторение помогает надолго закрепить навыки.



Каждая тема делится на несколько уровней, посвященных определенным группам навыков кибербезопасности. Уровни соответствуют угрозам разной степени опасности. Например, первого уровня достаточно для защиты от простейших и массовых атак, а для защиты от сложных и целевых атак необходимо освоить следующие уровни.

- Принцип «от простого к сложному»: знания растут с каждой новой темой и каждым новым уровнем
- Применение и развитие полученных ранее знаний в новых ситуациях

Разные виды контента

- На каждом уровне есть интерактивный урок, упражнения на закрепление навыков и проверку знаний (тест и имитация фишинговой атаки, если она требуется)
- Все элементы направлены на развитие конкретного навыка, которому посвящен урок, поэтому новые знания хорошо усваиваются и становятся частью новой модели поведения

Интервальное прохождение курса

- Кривая забывания Эббингауза: методы получения навыков кибербезопасности учитывают особенности человеческой памяти
- Повторение позволяет выработать привычки безопасного поведения и предотвращает забывание
- Знания закрепляются в каждом модуле

Темы тренингов

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

Пример: отработка навыков в рамках темы «Работа в интернете»

Базовый уровень Защита от массовых (дешевых и простых) атак	Начальный уровень Защита от массовых атак определенного профиля	Средний уровень Защита от хорошо подготовленных направленных атак	Продвинутый уровень* Защита от целевых атак
23 навыка, в том числе: – Распознавание поддельных всплывающих окон – Выявление перенаправляющих ссылок – Определение различий между подлинными и поддельными ссылками для скачивания – Распознавание исполняемых файлов, найденных в интернете – Умение определить подлинность расширения браузера	34 навыка, в том числе: – Ввод данных только на сайтах с действующим SSL-сертификатом – Использование разных паролей для разных учетных записей – Распознавание поддельных сайтов по ряду признаков – Отказ от перехода по числовым ссылкам – Распознавание недействительных адресов сетевых ссылок по поддельным поддоменам	14 навыков, в том числе: – Проверка ссылок для передачи файлов перед отправкой – Использование программ для торрентов только от проверенных производителей – Загрузка с торрентов только легального контента – Регулярное удаление файлов cookie браузера	13 навыков, в том числе: – Умение распознавать сложные поддельные ссылки (включая ссылки, похожие на адреса сайтов компании, и ссылки с перенаправлением) – Проверка сайтов с помощью специальных утилит – Выявление случаев, когда браузер занимается майнингом – Отказ от перехода на сайты с черным SEO
	+ Закрепление навыков начального уровня	+ Закрепление ранее полученных навыков	+ Закрепление ранее полученных навыков

Основные вопросы, рассматриваемые в теме: ссылки, загрузки, установка программ, регистрация и вход в учетную запись, онлайн-платежи, SSL

Сбалансированный структурированный контент, напрямую связанный с повседневной работой, как залог эффективности тренинга

Пример редактируемого фишингового сообщения для симуляции атаки и обратная связь

Принципы в Kaspersky Automated Security Awareness Platform учитывают специфику человеческого мышления, наши способности усваивать и запоминать информацию. Материалы включают множество реальных примеров, подчеркивающих важность соблюдения правил кибербезопасности сотрудниками. Платформа нацелена на формирование навыков, а не просто на информирование, поэтому в основе каждого модуля лежат практические упражнения и задачи, связанные с повседневной работой обучающихся.

Разные типы упражнений подогревают интерес к тренингу и мотивируют освоение навыков кибербезопасного поведения.

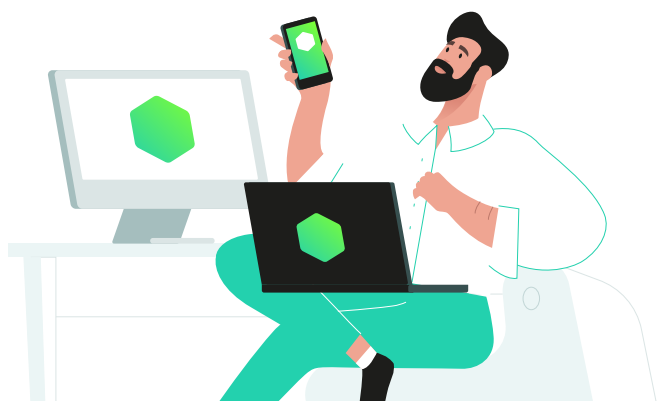
Графическое оформление и тексты не просто переведены на разные языки, но и адаптированы с учетом особенностей соответствующей культуры или региона.

Имитации фишинговых атак

Фишинговые кампании дополняют основную программу тренинга и позволяют проверить, насколько хорошо сотрудники умеют распознавать фишинг. Инструктор может определить пробелы в знаниях пользователей и посоветовать им темы для более глубокого изучения.

На платформе есть набор готовых шаблонов электронных писем для симуляции фишинга на всех поддерживаемых языках, и он регулярно обновляется. Вы также можете создать собственные письма на основе имеющихся шаблонов.

Попробуйте смоделировать фишинговую атаку еще до начала тренинга – посмотрите, справятся ли сотрудники. Это упражнение наглядно продемонстрирует пользу тренинга как самим сотрудникам, так и руководству.



Kaspersky Security Awareness – системный подход к тренингам в сфере IT-безопасности

Ключевые особенности программы

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.

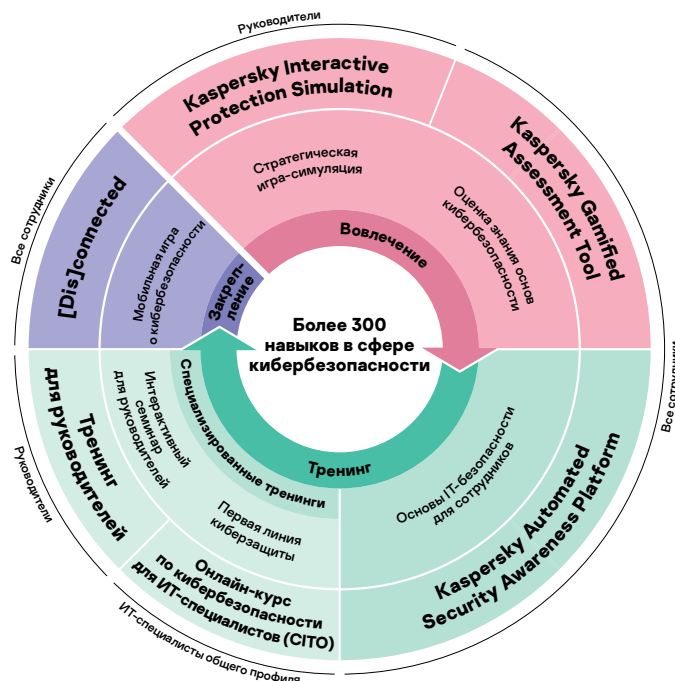
Глубокие знания в области кибербезопасности

Более 20 лет опыта в этой сфере легли в основу наших курсов

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.

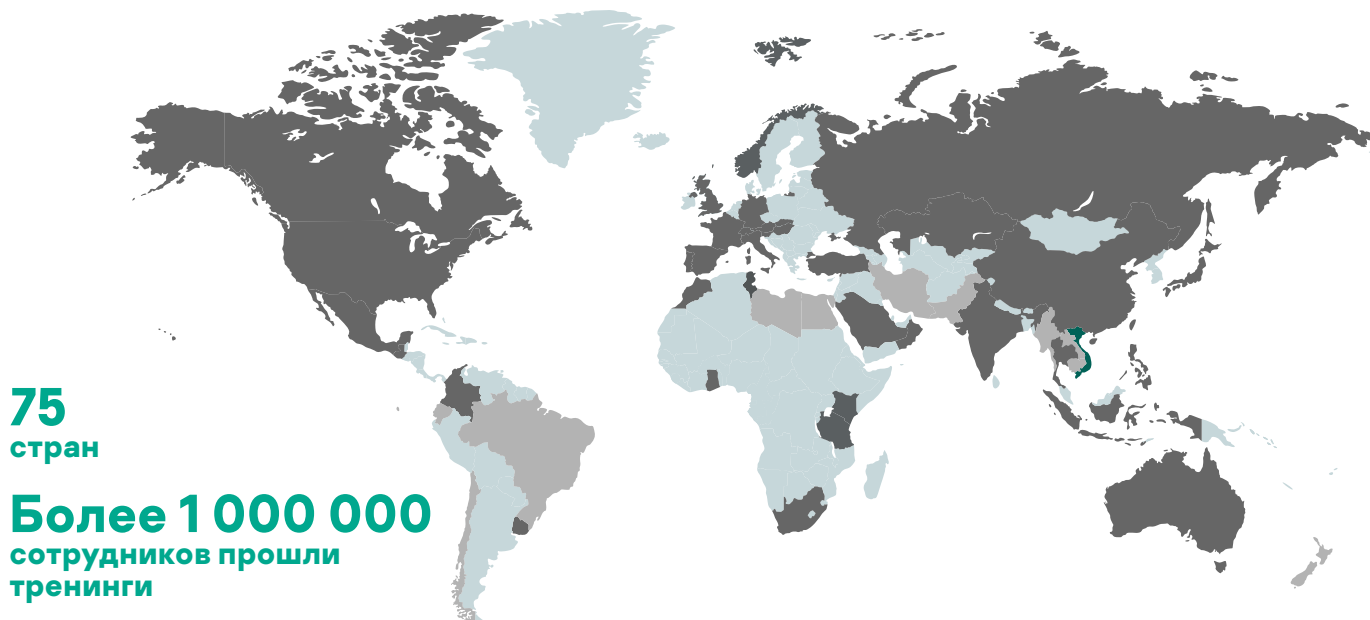
Подробная информация о пакетах тренингов на сайте: kaspersky.ru/awareness



Навыки, которые меняют поведение сотрудников на всех уровнях организации

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

Тренинги Kaspersky Security Awareness проходят по всему миру



Бесплатная пробная версия платформы: k-asap.ru
Kaspersky Automated Security Awareness Platform:
www.kaspersky.ru/small-to-medium-business-security/security-awareness-platform
Kaspersky Security Awareness: www.kaspersky.ru/awareness
Связаться с нами: Awareness@kaspersky.com

www.kaspersky.ru

kaspersky АКТИВИРУЙ
БУДУЩЕЕ