Эффективно для сотрудников.
Просто для руководителей.
Выгодно для компаний.

Kaspersky ASAP: Automated Security Awareness Platform

Бесплатная пробная версия
k-asap.ru

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky
Automated Security
Awareness Platform

Kaspersky Automated Security Awareness Platform

82% всех киберинцидентов вызваны человеческим фактором. В результате компании несут многомиллионные убытки. Традиционные тренинги не решают этой проблемы, поэтому необходим совершенно новый подход. И тут на помощь приходит Kaspersky Automated Security Awareness Platform.

Человеческие ошибки – основной источник киберрисков

79%
сотрудников компаний признались, что за предшествующий год совершили как минимум один неосторожный поступок, хотя заранее знали о связанных с ним рисках***

51%
сотрудников компаний считают, что вся ответственность за защиту бизнеса от кибератак лежит на сотрудниках IT-отделов*

55% компаний сообщили об инцидентах, вызванных ненадлежащим использованием информационных технологий их собственными сотрудниками**

51% предприятий малого бизнеса хотя бы раз пострадали от инцидентов безопасности, произошедших из-за нарушения сотрудниками политик ИТ-безопасности**

26% сотрудников компаний сообщили, что их пароли от личной и рабочей электронной почты 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

Обучение 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 прогресс обучения?

Как добиться заинтересованности сотрудников?

* Balancing Risk, Productivity, and Security («Баланс между риском, производительностью и безопасностью»), Delinea 2021 г.

** IT Security Economics 2022 («Экономика IT-безопасности за 2022 г.»), «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. Решение представляет собой онлайн-инструмент, цель которого – в течение года сформировать у сотрудников уверенные практические навыки кибергигиены, тем самым **сокращая количество киберинцидентов, связанных с человеческим фактором.**

Запуск и использование платформы не требуют специальных ресурсов и подготовки. На каждом этапе обучения, цель которого – формирование безопасной корпоративной киберсреды, учащимся помогают встроенные подсказки.

Полезный и содержательный контент

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, вобравшей в себя **более чем 25-летний опыт работы «Лаборатории Касперского» в области кибербезопасности**. Эта модель включает **более 350 важнейших практических навыков кибербезопасности**, которыми должен обладать каждый сотрудник.

Обучите ваших сотрудников навыкам кибербезопасности.
Измените их привычки и модели поведения и защитите IT-структуру вашего бизнеса.

Эффективность обучения

Систематизированное содержание	– Тщательно продуманный структурированный контент – Интерактивные уроки, постоянное закрепление материала, тесты 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 установления 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

Простота управления	– Полностью автоматизированное управление позволяет каждому сотруднику овладеть навыками кибербезопасности в соответствии с его профилем рисков без вмешательства администратора платформы – Синхронизация с AD (Active Directory), использование технологии единого входа SSO (Single Sign-On), взаимодействие со сторонними сервисами с помощью Open API, а также онлайн-помощь при первом входе, раздел FAQ и подсказки делают управление платформой удобным и эффективным
Простой контроль	Единая панель и актуальные отчеты: – отчеты о прохождении уроков – отчеты о прохождении тестов и имитаций фишинговых атак
Простота обучения	Платформа автоматически рассылает приглашения, напоминания и отчеты обучающимся и администраторам.

Варианты поставки

Kaspersky ASAP может поставляться в трех различных вариантах, в зависимости от ваших предпочтений:

- **Полностью онлайн облачное решение.** При этом обработка пользовательских данных осуществляется в полном соответствии с действующим законодательством, в зависимости от выбранного местоположения сервера. Например, если вы выберете Россию, Ваши данные будут храниться в Российской Федерации (Москва). Все охраняемые законом данные будут обрабатываться в соответствии с законодательством Российской Федерации.
- **Учебные модули в пакете SCORM.** Благодаря этой опции модули можно интегрировать с вашей собственной LMS (системой управления обучением). Но обратите внимание, что этот вариант не включает тесты и симуляцию фишинговых атак.
- **On-premise** (развертывания продукта в периметре сети организации). Этот вариант предназначен для клиентов, которым необходим максимальный уровень конфиденциальности. Для предприятий, связанных той или иной формой нормативного контроля, локальное развертывание обеспечивает соблюдение требований, что позволит избежать крупных штрафов и санкций. Разворачивая платформу обучения в собственной сети, вы имеете полный контроль над серверным оборудованием, безопасностью данных и конфигурацией. Пользователи могут получать доступ к обучающим материалам даже без подключения к интернету.

Управление платформой Kaspersky ASAP: простота благодаря полной автоматизации

Запуск программы в 4 шага

1

Добавьте пользователей

Пользователей можно добавлять, используя синхронизацию с **AD (Active Directory)**, загрузив файл .xlsx или в ручном режиме.

2

Разделите пользователей на группы

Разделите пользователей на группы вручную или автоматически в соответствии с целевым уровнем знаний.

3

Запустите обучающий курс

Разделите пользователей на группы вручную или автоматически в соответствии с целевым уровнем знаний и определите дату начала занятий для каждой группы.

4

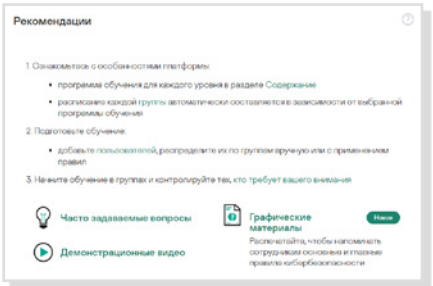
Автоматизированное управление обучением осуществляется платформой ASAP

Платформа ASAP составляет расписание для каждой группы, а также график отправки приглашений, напоминаний и прочих уведомлений. Все происходит автоматически.

Новейший усовершенствованный подход к обучению

Платформа Kaspersky ASAP предлагает новый способ предоставления учебных материалов по кибербезопасности. Можно либо назначить сотрудникам базовый экспресс-курс, который поможет быстро выполнить нормативные требования к обучению кибербезопасности или освежить их знания, либо выбрать основной курс, разбитый на несколько уровней сложности.

На главной странице портала для администратора есть все, что нужно для начала работы: помощь при первом входе в систему, полезные рекомендации, раздел FAQ и демо-ролики по использованию платформы с точки зрения администратора и пользователя.



Темы тренингов

Темы тренингов

Основной курс	Экспресс-курс
Электронная почта	Электронная почта
Пароли и учетные записи	Пароли и учетные записи
Веб-сайты и интернет	Веб-сайты и интернет
Социальные сети и мессенджеры	Защита мобильных устройств
Безопасность компьютера	Социальные медиа
Мобильные устройства	Мой компьютер
Защита конфиденциальных данных	Защита конфиденциальных данных
Личные данные	Доксинг
Общий регламент по защите данных (GDPR)	Безопасность криптокошельков
Промышленная кибербезопасность	Информационная безопасность удаленных рабочих мест
Безопасность платежных карт и стандарт безопасности PCI DSS	Федеральный закон "О защите персональных данных" № 152-ФЗ (для Российской Федерации)
Физическая безопасность данных	Федеральный закон “О безопасности критической информационной инфраструктуры Российской Федерации” № 187-ФЗ

* Полный список тем и понятий ищите на k-asap.com/ru

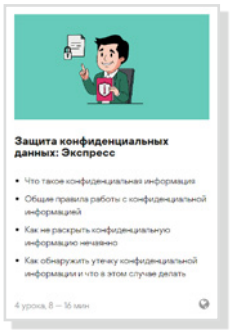
Темы разделены на большие блоки, включающие множество понятий из сферы IT-безопасности.*

#Пароли #Фишинг #Корпоративные учетные записи #Опасные сообщения #Банковские карты #Программы-вымогатели #Социальная инженерия #Опасные файлы #Работа в браузерах #Корпоративная этика #Антивирусное ПО #Вредоносное ПО #Приложения #Браузер #Конфиденциальная информация #Хранение информации #Отправка информации #Личные данные #Интернет и законодательство #Законодательство Евросоюза #Бизнес#Опасные ссылки #Поддельные вебсайты #сайты с программами-вымогателями#Резервное копирование #Мобильные данные #Шифрование #Облачные сервисы #Промышленный шпионаж #Стандарт PCI DSS #Двухфакторная аутентификация #Цифровой след #Торренты #Кэтфишинг #Целевая атака #Хэширование #Токены #Шаблоны блокировки экрана #Майнинг #Родительский контроль

Каждая тема состоит из нескольких уровней, посвященных определенным навыкам кибербезопасности. Уровни соответствуют угрозам разной степени опасности. Например, первого уровня достаточно для защиты от простейших и массовых атак. Для защиты от наиболее изощренных и целевых атак необходимо освоить более продвинутые уровни.

Пример. Навыки, приобретаемые при обучении по теме «Веб-сайты и Интернет»

Начальный уровень Защита от массовых (дешевых и простых) атак	**Базовый уровень** Защита от массовых атак определенного профиля	**Средний уровень** Защита от хорошо подготовленных целевых атак	**Продвинутый уровень*** Защита от целевых атак
23 навыка, включая: – 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, включая:** – 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	**12 навыков, включая:** – 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, включая:** – 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 базовых навыков	+ Закрепление ранее полученных навыков	+ Закрепление ранее полученных навыков

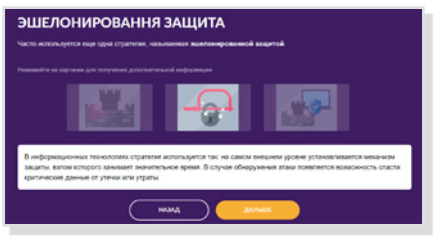


Экспресс-курс Kaspersky Automated Security Awareness Platform

Краткая версия тренинга в аудио и видео формате. Каждая тема состоит из нескольких коротких уроков, направленных на освоение базовых навыков кибербезопасности.

- Интерактивная теоретическая часть
- Видео
- Тесты

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

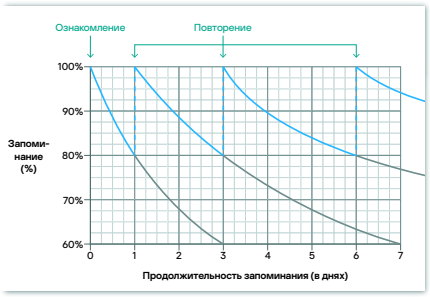


Основной курс Kaspersky Automated Security Awareness Platform

Этот курс разработан с учетом специфики человеческой памяти.

- Разные виды контента
  - Каждый учебный модуль включает интерактивный урок, упражнения на закрепление навыков и проверку знаний (тест и имитация фишинговой атаки, если это требуется).
  - Все эти элементы направлены на развитие конкретного навыка, которому посвящен модуль, поэтому новые знания хорошо усваиваются и становятся частью новой модели поведения.

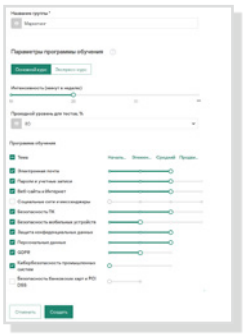
Кривая Эббингауза («кривая забывания»)



- Интервальное прохождение курса
  - Отдельные элементы тренинга следуют друг за другом с определенными интервалами, что предотвращает быстрое пролистывание уроков и улучшает запоминание. Интервалы рассчитаны с учетом «кривой забывания» Эббингауза.
  - Повторение позволяет выработать привычки безопасного поведения и предотвращает забывание.

- Сбалансированный структурированный контент, напрямую связанный с повседневной работой, как залог эффективности тренинга
  - Материалы включают множество реальных примеров, подчеркивающих важность соблюдения правил кибербезопасности для каждого.
  - Основное внимание уделяется отработке навыков, а не просто предоставлению знаний, поэтому в основе каждого модуля лежат практические упражнения и задачи для сотрудников.

Гибкий учебный план

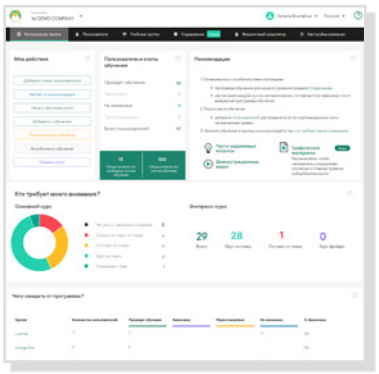


Гибкость программы обучения

В платформе реализован гибкий подход к тренингу, процессом последовательно и автоматизированно управляет сама платформа. Для каждой учебной группы можно выбрать:

- основной курс, экспресс-курс или их комбинацию;
- темы для изучения в группе в рамках основного курса и экспресс-курса;
- целевой уровень знаний по каждой выбранной теме основного курса.

На основе этого выбора платформа автоматически выстроит учебный процесс для каждой группы.



Управляйте тренингом с помощью удобной панели управления

- Получить все необходимое для управления тренингом – статистику, отчеты о действиях и прогрессе участников, информацию о доступных слотах, групповых занятиях, предложения по улучшению результатов – можно через единую панель управления. Отчеты загружаются одним щелчком мыши. Частоту получения отчетов также можно настроить.

Независимое обучение

- Сотрудники могут проходить тренинги в любое удобное время и на любом устройстве, поскольку платформа Kaspersky ASAP адаптирована для мобильных устройств. Это делает обучение простым и удобным.
- Пользователи получают доступ к учебной платформе через персональную ссылку, полученную в приглашении на тренинг, или через общую ссылку, если администратор настроил единый вход SSO (Single Sign-On).

Дополнительные настройки

Администратор может легко поменять внешний вид платформы:

- заменить логотип «Лаборатории Касперского» на логотип своей компании на панели администратора, на учебном портале и в шаблоне электронных писем;
- персонализировать сертификаты;
- добавлять персонализированный контент в любой урок.

Платформа Kaspersky ASAP может быть интегрирована с платформами Kaspersky Unified Monitoring and Analysis (KUMA) и Extended Detection and Response (XDR).
– Администратор может увидеть событие в XDR и предпринять соответствующие меры, в том числе направить сотрудника на тренинг на платформу ASAP.
– В карточку инцидента можно автоматически добавлять информацию об уровне киберграмотности сотрудника, подвергшегося атаке.

* Полный список поддерживаемых языков ищите на k-asap.com

Интеграция

С помощью Open API платформа может взаимодействовать со сторонними сервисами. Open API работает через протокол HTTP и предлагает набор методов запроса/ответа.

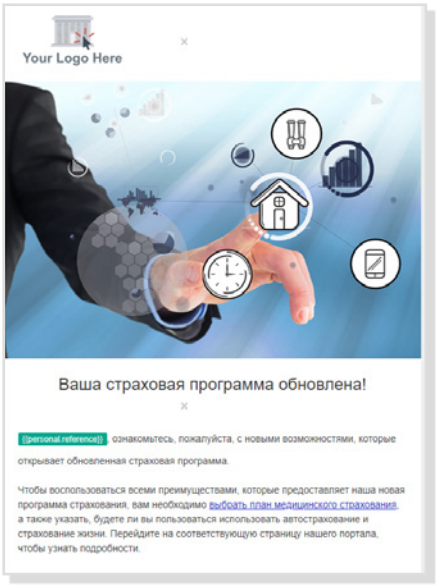
Локализация

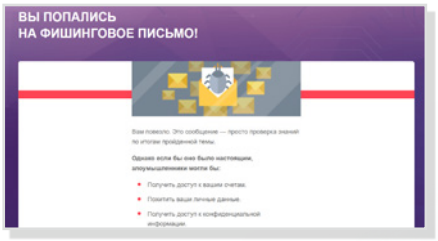
Kaspersky ASAP поддерживает 25 языков*. Локализация платформы выходит за рамки обычного перевода. Текст и изображения не просто переведены на разные языки, они адаптированы к местным культурам и реалиям.

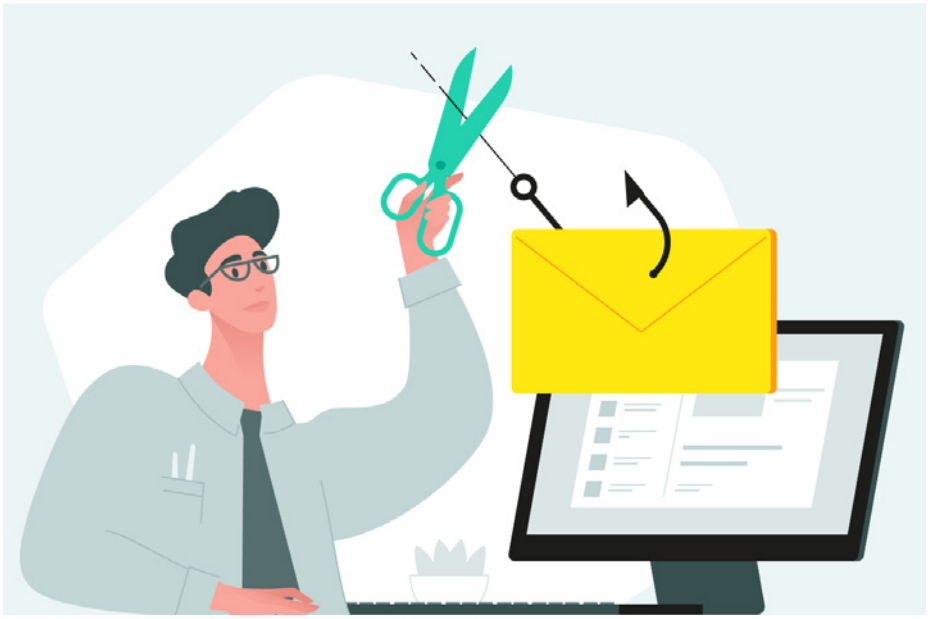
Имитации фишинговых атак

Фишинговые кампании дополняют основную программу тренинга. Они позволяют проверить, насколько хорошо сотрудники умеют распознавать фишинг, и помогают инструкторам быстро найти пробелы в знаниях пользователей и мотивировать их на более глубокое изучение проблемных тем. Фишинговые кампании – это превосходный инструмент для обучения сотрудников навыкам распознавания потенциально опасных ситуаций и применению этих навыков на практике.
Платформа содержит готовые шаблоны фишинговых писем на всех поддерживаемых языках. Эти шаблоны регулярно обновляются и добавляются новые. Также можно создавать собственные письма на основе имеющихся шаблонов.

Пример редактируемого фишингового сообщения для симуляции атаки и ответная реакция







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

Сотрудники могут продемонстрировать свое понимание темы, не попавшись на имитацию атаки и сообщив о фишинговых письмах с помощью инструмента **«Сообщить о фишинге»**.

Инструмент «Сообщить о фишинге» удаляет письмо из папки «Входящие» и отправляет уведомление не только администратору платформы, но и сотрудникам IT- и ИБ-отделов. Таким образом сотрудник подтверждает высокий уровень своей киберграмотности, а организация повышает уровень обнаружения фишинговых угроз и реагирования на них.

Kaspersky ASAP для партнеров MSP/MSSP или компаний с территориально-распределенной структурой

Платформа позволяет вам развертывать и управлять обучением в нескольких компаниях сразу из-под одного аккаунта, с единой консоли, готовой к многопользовательской работе, без необходимости использования дополнительного программного обеспечения.

Хорошие новости! В Kaspersky ASAP есть функция управления пулом лицензий, которая позволяет назначать квоту лицензий для каждой компании с определенным сроком действия.

Также можно добавить дополнительных администраторов для каждой компании и назначить им разные роли.

Kaspersky Security Awareness – новый подход к освоению навыков ИТ-безопасности

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.

Обучение, меняющее поведение сотрудников всех должностей 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.

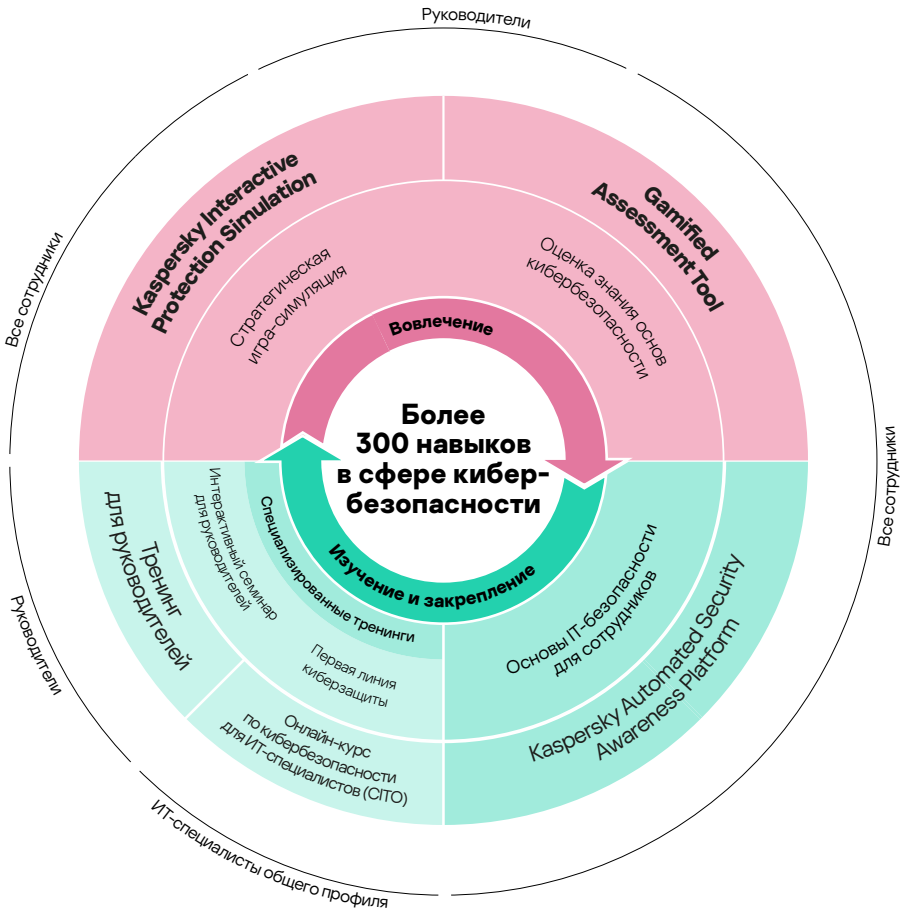
Kaspersky ASAP – ключевой элемент программы тренингов Kaspersky Security Awareness.

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.

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 высшее руководство 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 IT-безопасности: business.kaspersky.ru

www.kaspersky.ru

kaspersky **АКТИВИРУЙ БУДУЩЕЕ**