

**Kaspersky Automated Security Awareness Platform (ASAP):
автоматизированная платформа для повышения
осведомленности о кибербезопасности**

www.kaspersky.ru

#истиннаябезопасность

Kaspersky ASAP: автоматизированная платформа для повышения осведомленности о кибербезопасности

Предприятия теряют огромные средства, восстанавливая ресурсы после нарушений безопасности, вызванных действиями сотрудников. Однако традиционные программы обучения, призванные предотвращать такие инциденты, недостаточно эффективны. Обычно они не вдохновляют участников и не позволяют сформировать у них требуемое поведение.

Человеческий фактор как основной киберриск

83 000 долл. США для компаний малого и среднего бизнеса

Средний ущерб от атак, связанных с неосторожностью или неосведомленностью сотрудников ¹

101 000 долл. США на предприятие для компаний малого и среднего бизнеса

Ущерб от атак, связанных с фишингом и применением социальной инженерии ¹

400 долл. США на сотрудника в год

Средний ущерб от фишинговых атак (без учета других типов киберугроз)

52% всех организаций

Считают неосторожность сотрудников (пользователей) главной проблемой в стратегии обеспечения IT-безопасности ¹

¹ Данные исследования «Информационная безопасность бизнеса», проведенного «Лабораторией Касперского» весной 2018 года. В опросе приняли участие 6614 IT-специалистов из 29 стран по всему миру, включая Россию.

² Данные взяты из исследования Cost of Phishing and Value of Employee Training (Ущерб от фишинга и значимость обучения сотрудников), институт Ponemon, август 2015 г.

Барьеры для эффективного повышения осведомленности о кибербезопасности

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

Даже организации, в которых повышением осведомленности сотрудников



Непонятно, как ставить цели и планировать обучение



Организация обучения отнимает слишком много времени



Отчетность не помогает следить за достижением целей



Сотрудники недовольны программой → не получают навыки

занимаются выделенные рабочие группы, испытывают трудности.

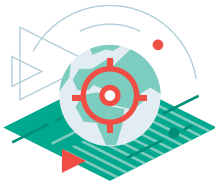
Как правило, компании выбирают один из двух вариантов: проводят разовые занятия (например, «Кибербезопасность за 1 час») или хорошо структурированные профессиональные обучающие программы, из которых однако используют лишь некоторые базовые функции и инструменты: несколько волн симулированных фишинговых атак в течение года и пара обзорных уроков. Полный курс обучения оказывается слишком сложно организовать. Как результат — в обоих случаях сотрудники не получают навыков, необходимых для обеспечения кибербезопасности организации.

Простое и эффективное повышение осведомленности для компаний любого размера

«Лаборатория Касперского» представляет собственную автоматизированную платформу для повышения осведомленности о кибербезопасности – Kaspersky Automated Security Awareness Platform (ASAP).

Платформа представляет собой онлайн-инструмент, формирующий и закрепляющий у сотрудников навыки безопасной работы. Курс рассчитан на год. Удобный функционал и автоматизация процесса помогает компаниям на всех этапах: от постановки цели до оценки эффективности.

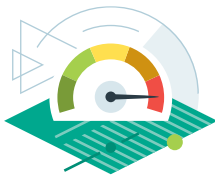
Шаг 1.



Постановка целей и обоснование необходимости повышения осведомленности

- Ставьте цели, опираясь на рекомендации.
- Стремитесь к балансу между желаемым уровнем киберосведомленности отдельных групп сотрудников и временем, необходимым для его достижения.

Шаг 2.



Формирование у каждого сотрудника навыков, соответствующих потребностям

- Используйте автоматизированное управление: платформа определяет набор навыков, необходимых определенному сотруднику, в соответствии с его профилем риска и выстраивает график прохождения программы.
- Будьте уверены, что полученные навыки будут использоваться благодаря тщательной проработке и закреплению материала.
- Повышайте осведомленность сотрудников в комфортном для них темпе с учетом их уровня риска и интенсивности программы, что позволит избежать переутомления, а, следовательно, и нежелания продолжать занятия.

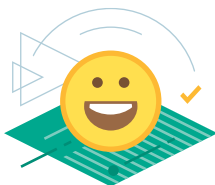
Шаг 3.



Отчетность и аналитика как инструменты отслеживания прогресса

- Оперативно отслеживайте изменения, тенденции и прогнозы.
- Пользуйтесь прогнозами в режиме реального времени: с их помощью вы сможете оценить и своевременно предпринять меры для достижения целей.
- Действуйте на опережение. Система сама подскажет, на какие подразделения или отдельных сотрудников нужно обратить внимание, чтобы достигнуть намеченной цели.

Шаг 4.



Мотивация – залог эффективности

- Наглядные задания, применимые к повседневной работе сотрудников.
- Персонализированный подход – сотрудники получают только необходимые знания в удобном для них темпе.

Простое управление благодаря автоматизации

Начните всего за 10 минут

- Добавьте пользователей в платформу и разделите их на группы в зависимости от желаемого целевого уровня обучения.
- Запустите занятия. Платформа сама выстроит график обучения для каждой группы и отправит пользователям приглашения.

Платформа построит процесс в соответствии с темпом и способностями сотрудников

- Платформа не предложит сложные темы прежде, чем пользователь освоит основы и успешно сдаст тест.
- Ответственному за обучение менеджеру не нужно тратить время на анализ результатов каждого сотрудника и подстройку программы.

Используйте разные программы для разных профилей риска

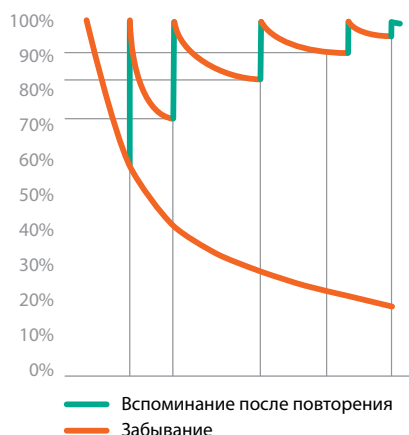
- Используйте правила, чтобы автоматически определять сотрудников в группы с разным целевым уровнем и интенсивностью в зависимости от их уровня доступа к конфиденциальной информации и специфики работы.
- Вы можете использовать готовые группы или создавать и настраивать их самостоятельно.

Вы сможете получать подробные отчеты в любое время

- В панели управления представлена вся необходимая информация для оценки прогресса.
- Платформа порекомендует вам, что нужно сделать, чтобы улучшить результат.

Кривая Эббингауза (кривая забывания)

Многочратное повторение помогает надолго закрепить навыки



От простого к сложному

Отработка навыков основана на принципе «от простого к сложному». Через 4 дня после прохождения теоретической части платформа автоматически рассылает письма с напоминанием пройденного материала, а еще через 3 дня предлагает пройти тест – проверку полученных знаний. Если тест пройден успешно, то через некоторое время пользователь получит письмо с симулированной фишинговой атакой. Такой подход обеспечивает надежное закрепление навыков и препятствует забыванию.

Учимся понемногу

- Программа специально разбита на короткие занятия (от 2 до 10 минут), потому что длинные и скучные уроки могут утомить ваших сотрудников.

Полный набор инструментов для всех областей безопасности

- Каждый уровень включает: интерактивный модуль и видео → упражнения на закрепление → проверку (тест или имитацию фишинговой атаки)

Каждая тема делится на несколько уровней, посвященных отработке определенной группы навыков в сфере безопасности. Уровни соответствуют угрозам разной степени опасности: первого уровня достаточно для защиты от простейших и массовых атак, а для защиты от сложных и целевых атак необходимо изучить более продвинутые уровни.

Темы*

Электронная почта и фишинг

Работа в интернете

Пароли

Социальные сети и службы обмена сообщениями

Безопасность компьютеров

Безопасность компьютеров

Мобильные устройства

Конфиденциальные данные

Общоевропейские нормативы защиты данных (GDPR)

Социальная инженерия

Пример: отработка навыков в рамках темы «Интернет»

Начальный уровень: защита от массовых (простых) атак	Базовый уровень: защита от массовых атак определенного профиля	Средний уровень: защита от хорошо подготовленных атак	Продвинутый уровень: защита от целевых атак
<p>13 навыков, в том числе:</p> <ul style="list-style-type: none"> – настройка компьютера (обновления, антивирус) – умение распознавать явно вредоносные веб-сайты (то есть сайты, на которых предлагают обновить ПО, ускорить работу компьютера, отправить SMS, установить проигрыватели и т. д.) – привычка не открывать исполняемые файлы с веб-сайтов 	<p>20 навыков, в том числе:</p> <ul style="list-style-type: none"> – регистрация и вход в учетную запись только на надежных сайтах – отказ от перехода по числовым ссылкам – ввод конфиденциальной информации только на надежных сайтах – умение распознавать признаки вредоносных веб-сайтов 	<p>14 навыков, в том числе:</p> <ul style="list-style-type: none"> – умение распознавать поддельные ссылки – умение распознавать вредоносные файлы и загрузки – умение распознавать вредоносное ПО 	<p>13 навыков, в том числе:</p> <ul style="list-style-type: none"> – умение распознавать сложные поддельные ссылки (включая ссылки, похожие на адреса сайтов вашей компании, и ссылки с перенаправлением) – отказ от перехода на сайты с черным SEO – выход из учетной записи после окончания работы – продвинутая настройка компьютера (отключение Java, блокировка рекламы, использование надстроек и т. д.)
	+ закрепление навыков начального уровня	+ закрепление ранее полученных навыков	+ закрепление ранее полученных навыков

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

* Окончательный состав тем может быть изменен без предупреждения.

Игровой формат и актуальные темы

В основе обучения лежит симуляция реально происходящих на практике событий и личная значимость кибербезопасности для сотрудников. Цель платформы – сформировать навыки, а не только передать знания, поэтому практические задания – неотъемлемый компонент каждого модуля.

Различные типы упражнений подогревают интерес пользователей к обучению и мотивируют их на освоение навыков безопасного поведения.

Метод симуляции позволяет формировать практические навыки и одновременно поддерживать интерес и мотивацию пользователей

The screenshot displays a simulated email inbox titled "Пути распространения" (Distribution Paths). The selected email is from "Google Accounts - новая политика конфиденциальности" (new@googlerprivacypolicy.org) with the subject "Политика конфиденциальности.zip". The body of the email contains a warning about a new privacy policy and a link to a zip file. To the right, a dark overlay window shows a security alert: "Письма с вложениями – основной путь распространения программ-вымогателей. Ответьте на несколько вопросов, находясь в почтовом клиенте Марии." (Attachments – the main way of spreading ransomware. Answer a few questions while in the Maria email client). Below this, a question asks: "Откройте письмо 'Google Accounts'. Оно действительно пришло от Google?" (Open the 'Google Accounts' email. Did it really come from Google?). The user has selected "еже-файлы" (every-files) and is presented with "ДА" (Yes) and "НЕТ" (No) buttons.

The screenshot shows a quiz question: "Как вы думаете, сколько времени нужно вирусу, чтобы зашифровать ваши файлы?" (How do you think, how long does it take a virus to encrypt your files?). The options are: 30 минут (30 minutes), 1 час (1 hour), 3 часа (3 hours), and 10 часов (10 hours). The "30 минут" option is selected. Below the options, explanatory text states: "В среднем менее часа. Время зависит от объёма данных на вашем жёстком диске. Именно поэтому важно знать, как избежать заражения и сохранить свои данные." (On average, less than an hour. Time depends on the volume of data on your hard drive. That's why it's important to know how to avoid infection and save your data.). A "ДАЛЕЕ" (Next) button is at the bottom.

The screenshot shows a quiz question about user habits. The first part asks "Я пользуюсь:" (I use:) with a list of items: "Корпоративная сеть" (checked), "Браузер" (checked), "Электронная почта" (checked), and "Съёмные носители (флешки, внешние жёсткие диски)" (unchecked). The second part asks "А также:" (Also:) with a list of habits: "Я посещаю сайты с бесплатными софтом, музыкой, онлайн-кинотеатры, торрент-трекеры" (checked), "Я не пользуюсь антивирусом" (unchecked), "Я откладываю обновления операционной системы, браузера" (checked), and "Я пропускаю антивирусную проверку при подключении съёмного носителя" (checked). Below the list, a text box states: "Вероятность проникновения программы-вымогателя на ваш компьютер – высокая. Рекомендуем внимательно изучить материал урока, чтобы не стать жертвой мошенников." (The probability of ransomware infection on your computer is high. We recommend you carefully study the lesson material to avoid becoming a victim of scammers.). A "ДАЛЕЕ" (Next) button is at the bottom.

до **90%**

сокращение общего количества инцидентов

не менее **50%**

снижение финансового ущерба от инцидентов

до **93%**

вероятность применения полученных навыков в повседневной работе

более чем **30-кратная**

окупаемость инвестиций в безопасность

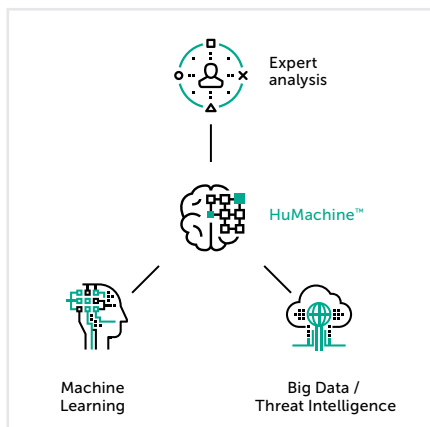
рекордные **86%**

участников готовы рекомендовать платформу



Kaspersky® Security Awareness

Автоматизированная платформа для повышения осведомленности о кибербезопасности – один из компонентов Kaspersky Security Awareness. Этот продукт включает в себя программы компьютерного обучения для представителей различных структурных подразделений и должностей.



«Лаборатория Касперского»

www.kaspersky.ru

#истиннаябезопасность
#HuMachine

© АО «Лаборатория Касперского», 2019. Все права защищены. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью соответствующих владельцев.