Kaspersky
Security
Awareness

Создание культуры киберграмотности для защиты вашего бизнеса

kaspersky активируй будущее

Эффективный подход к снижению рисков, связанных с поведением пользователей

Почему внедрение культуры киберграмотности так важно? Сотрудники ошибаются, компании теряют деньги.

> Общий уровень зрелости определяется не средним значением, а самым слабым звеном системы. Даже при наличии сильных сторон один-единственный критический пробел может свести на нет все усилия по обеспечению кибербезопасности.

64%

Большинство инцидентов кибербезопасности вызвано человеческим фактором[1]

4,4 млн долларов

в среднем составляет ущерб организаций от кибератак[2]

Создание культуры киберграмотности приносит ощутимый результат

По данным «Лаборатории Касперского», 87,2% респондентов, прошедших тренинг, отметили изменения в поведении, стали более внимательными и осторожными.

Kasperky Security Awareness: создайте устойчивую культуру безопасности на всех уровнях

Поскольку устойчивые изменения в поведении требуют времени, наш подход подразумевает построение непрерывного образовательного процесса с использованием различных инструментов и материалов для закрепления изученного.

92%

пользователей рекомендуют эти тренинги другим

3 млн

сотрудников успешно прошли обучение

160+

стран — география использования

Почему клиенты выбирают Kaspersky Security Awareness?

> Наши эксперты одними из первых в мире обнаруживают новые угрозы — мы обучаем ваших сотрудников их распознавать.

30 лет опыта и экспертизы в области кибербезопасности

Обучение, которое меняет поведение сотрудников на всех уровнях организации

1 Отчет «Лаборатории Касперского» Human Factor 360 («Человеческий фактор»), отчеты Cybersecurity Ventures и Verizon о киберинцидентах.

2 Cost of a Data Breach Report 2025 («Ущерб от утечки данных в 2025 году»). IBM, 2025 г.

Kaspersky Automated Security Awareness Platform (KASAP)

KASAP — ключевой компонент Kaspersky Security Awareness.

Это интерактивная онлайн-платформа с увлекательными уроками, которые вырабатывают навыки кибербезопасного поведения.

Формат, который подойдет любой компании, независимо от ее размера и требований. On-premise решение для компаний с повышенными требованиями к информационной безопасности. Возможность добавлять свой контент в формате PDF и SCORM.

KASAP – это не просто инструмент для защиты от фишинга. Используя матрицу MITRE ATT&CK, платформа наглядно показывает сотрудникам, какие типы атак они могут предотвратить и как. Примеры:

Техника MITRE	Угроза	Новые навыки и привычки
T1566. Фишинг	Вредоносные письма	Распознавание фишинговых атак и информирование руководства и IT-служб о них
T1585. Создание учетных записей	Поддельные учетные записи и профили	Подтверждение личности собеседника перед раскрытием информации
T1199. Доверительные отношения	Злоупотребление доверием партнера	Проверка нетипичных запросов
T1091. Распространение через съемные носители	Съемные носители	Распознавание вредоносных программ на USB-устройствах
T1078. Использование существующих учетных записей	Кража учетных данных	Распознавание методов социальной инженерии, используемых для получения доступа

Основной курс — 39 модулей по базовым темам

Экспресс-курс — короткие интерактивные модули по 20 темам

Ключевые темы:

- Искусственный интеллект и нейросети
- Атаки на цепочку поставок
- Культура киберграмотности
- Вишинг: борьба с телефонными мошенниками
- Атаки на топ-менеджмент и от имени топ-менеджеров
- Электронная почта
- Пароли и учетные записи
- Веб-сайты и интернет
- Безопасность компьютера
- Защита конфидециальных данных
- Личные данные
- Физическая безопасность данных
- Общий регламент по защите данных (GDPR)
- Социальные сети и мессенджеры
- Мобильные устройства
- Промышленная кибербезопасность
- Реагирование на инциденты
- Безопасность платежных карт и стандарт безопасности PCI DSS

95 %

сотрудников, прошедших курсы вооружены навыками по защите от от фишинговых атак

в 20 раз

меньше утечек при соблюдении цикла комплексного обучения[1]

Попробовать бесплатно

1 Исследование Kaspersky Automated Security Awareness Platform, 2025 г.

Возможности KASAP

1

Кибербезопасное поведение

Множество тем и более 500 практических навыков. Гибкая программа, доступная более чем на 30 языках

2

Симулятор фишинга

Настраиваемые шаблоны фишинговых атак: ссылки, вложения, QR-коды, плагин «Сообщить о фишинге»

3

Удобное управление программой

Мгновенное развертывание, Open API, интеграция с Active Directory и службой единого входа, возможности персонализации, мультитенантность

4

Управление рисками на основе расширенной аналитики

Интеграция с Kaspersky SIEM и XDR

План занятий

Модульная подача материала с чередованием видов деятельности повышает эффективность запоминания

Результаты:

1

Сокращение количества инцидентов, связанных с человеческим фактором

2

Минимизация репутационного ущерба

3

Снижение риска юридической ответственности и штрафов — формирование культуры безопасности в соответствии с нормативными требованиями (GDPR. PCI DSS и другие стандарты обработки и защиты данных)

4

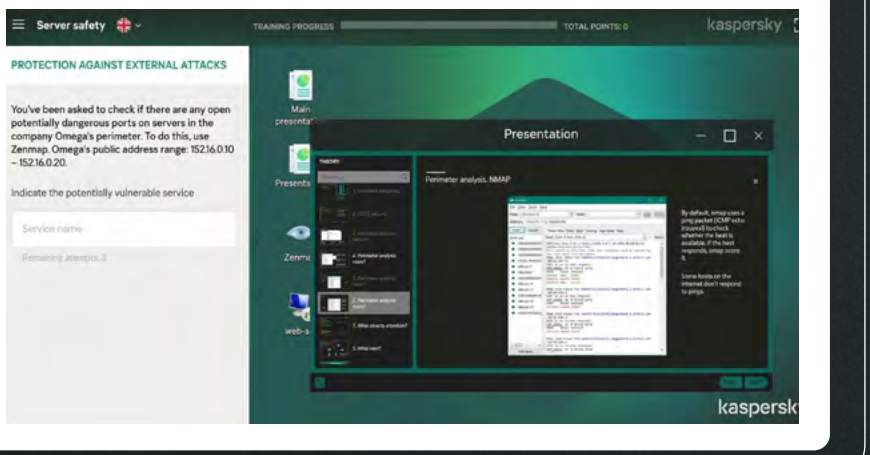
Сокращение времени, затрачиваемого на проведение тренингов по повышению осведомленности, и уменьшение нагрузки на ИТ-команду

Kaspersky Cybersecurity for IT Online

ИТ-специалисты получат практические навыки распознования потенциального сценария атаки в, казалось бы, безобидном инциденте и узнают, как собрать данные об инцидентах для передачи команде ИТ-безопасности.

ИТ-специалисты узнают, как:

- Обнаружить вредоносное ПО, потенциально нежелательное ПО, эксплойты и фишинговые атаки, провести анализ и принять ответные меры
- Использовать нужные инструменты и техники для усиления защиты информационной инфраструктуры и эффективного расследования инцидентов
- Анализировать журналы, собирать цифровые улики и расследовать инциденты
- Усиливать защиту, настраивать политику и мониторинг для повышения безопасности серверов и Active Directory



6 модулей, более 30 практических занятий

Вредоносные программы	Потенциально нежелательные программы и файлы	Безопасность сервера
Основы расследования инцидентов	Реагирование на фишинговые атаки	Безопасность Active Directory

Kaspersky Executive Training

Руководители владеют ценными данными, поэтому чаще других становятся целью злоумышленников. Знание основ информационной безопасности поможет топ-менеджерам не попасться на уловки и сохранить важную информацию.

Курс сосредоточен на ключевых и бизнес-аспектах кибербезопасности на доступном, нетехническом языке

- Обеспечивает понимание кибер-безопасности как части бизнес-системы
- Показывает, как киберриски влияют на бизнес и как ими можно управлять
- Основывается на глубоком знании потребностей топ-менеджеров
- Объясняет роль топ-менеджеровв кибербезопасности

Kaspersky Interactive Protection Simulation (KIPS)

Командная игра, которая показывает кибербезопасность с точки зрения бизнеса. Задача: принимать стратегические решения, которые помогут защитить компанию от кибератак и поддержать прибыльность бизнеса.

Формирование единого видения у ответственных лиц

Визуализация рисков кибер-безопасности и их влияния на прибыльность и эффективность бизнеса

Привлечение всех подразделений к решению вопросов кибер-безопасности и формирование культуры безопасного поведения

Офлайн-формат:

Интерактивная игра, которую можно провести как отдельное мероприятие или включить в программу конференции, семинара или корпоративного события.

- До 100 участников, 4–5 человек в команде
- Ведущий и ассистент на площадке

Онлайн-формат:

Идеально подходит для международных организаций и массовых мероприятий. Его можно комбинировать с офлайн-форматом — тогда в игре смогут участвовать как присутствующие, так и удаленные команды.

- До 300 команд (1000 участников) из любой точки мира

14 отраслевых сценариев

(список постоянно пополняется)

- ИТ
- Аэропорт
- Корпорация
- Банк
- Нефтегазовая компания
- Транспортная компания
- Электростанция
- ГЭС
- Орган местного самоуправления
- Нефтехимическое предприятие
- Нефтяной холдинг
- Малый и средний бизнес
- Телекоммуникационная компания
- Атрибуция кибератак

Персонализируйте игру под свои задачи:

- Игровые доски, карточки и номера столов с вашим или совместным брендингом
- Уникальный сценарий, разработанный в сотрудничестве с «Лабораторией Касперского», который может точно учитывать особенности вашей сети, прошлые инциденты или специфичные для отрасли угрозы

Формирование культуры киберграмотности

Из чего складывается культура киберграмотности?

- Поведение и привычки сотрудников
- Позиция руководства и согласованность в действиях руководителей разных уровней
- Интеграция безопасности в рабочие процессы
- Инфраструктурная и технологическая подготовленность

Внедрение культуры киберграмотности — это фундаментальное изменение подхода, которое делает работу эффективнее и спокойнее.

Чтобы безопасность всегда была в фокусе внимания сотрудника, нужна постоянная, методичная поддержка обучения:

Как определить уровень киберкультуры в вашей организации?

В настоящее время можно отметить, что количество жалоб на фишинговые сообщения значительно возросло, что можно расценивать как индикатор повышения уровня грамотности в области кибербезопасности.

Игорь Якутович

Начальник центра ИБ ГУП «Петербургский метрополитен»

Высокий уровень кибербезопасности является важнейшим приоритетом в осуществлении коммерческой деятельности нашей компании. Реализация непрерывного процесса повышения осведомлённости работников компании в вопросах кибербезопасности через Kaspersky Automated Security Awareness Platform — часть нашей стратегии усиления ИБ в ответ на новые угрозы, — комментирует представитель «ФосАгро». — Мы доверяем профессиональному подходу экспертов «Лаборатории Касперского» как в вопросе выбора тем, так и в плане организации учебного процесса.

Начните формировать культуру киберграмотности вместе с нами!

Попробовать KASAP бесплатно

Kaspersky Security Awareness

Ваша команда –
ваша защита!

www.kaspersky.ru

#kaspersky
#активируйбудущее