

Создание культуры
киберграмотности
для защиты вашего
бизнеса



kaspersky активируй
будущее

Сотрудники ошибаются – компании теряют деньги

64%

Большинство инцидентов
кибербезопасности вызвано
человеческим фактором¹

4,4 млн
долларов

Средний ущерб организации в
результате кибератаки²

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.

Вооружите сотрудников необходимыми навыками.
И тогда они станут настоящими киберзащитниками
вашей компании.



Примеры атак, связанных
с человеческим фактором,
из базы MITRE ATT&CK



Кибератаки



T1566	Фишинг
T1598	Фишинг с целью сбора сведений
T1091	Репликация при помощи съемных носителей
T1199	Доверительные отношения
T1585	Создание учетных записей

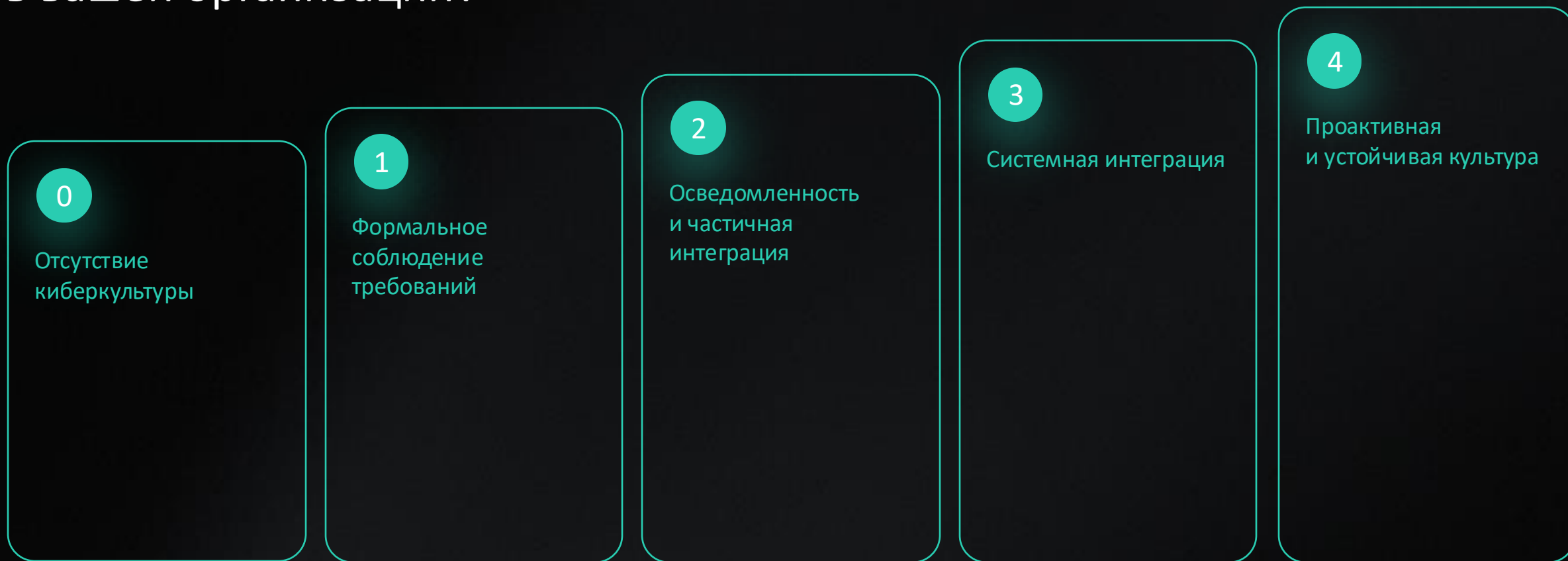


Конфиден-
циальные
данные



Как сделать безопасность
естественной частью
корпоративной культуры?

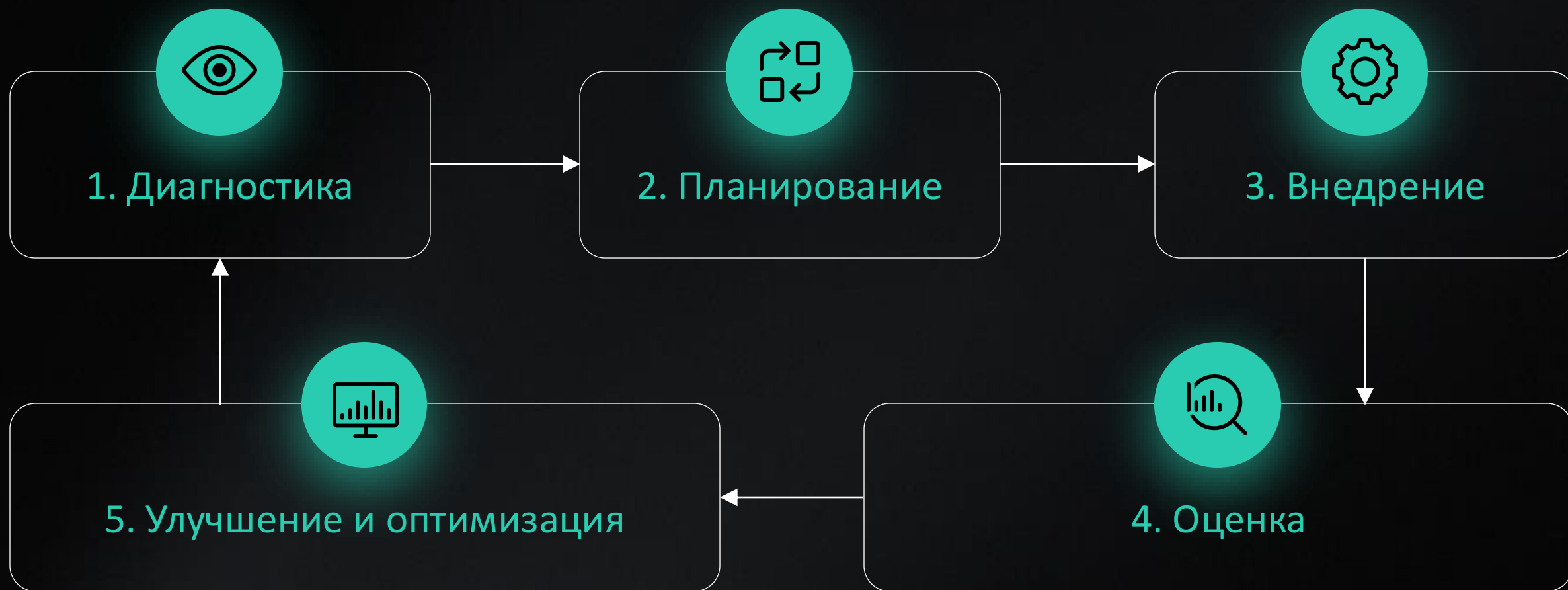
Как определить уровень киберкультуры в вашей организации?



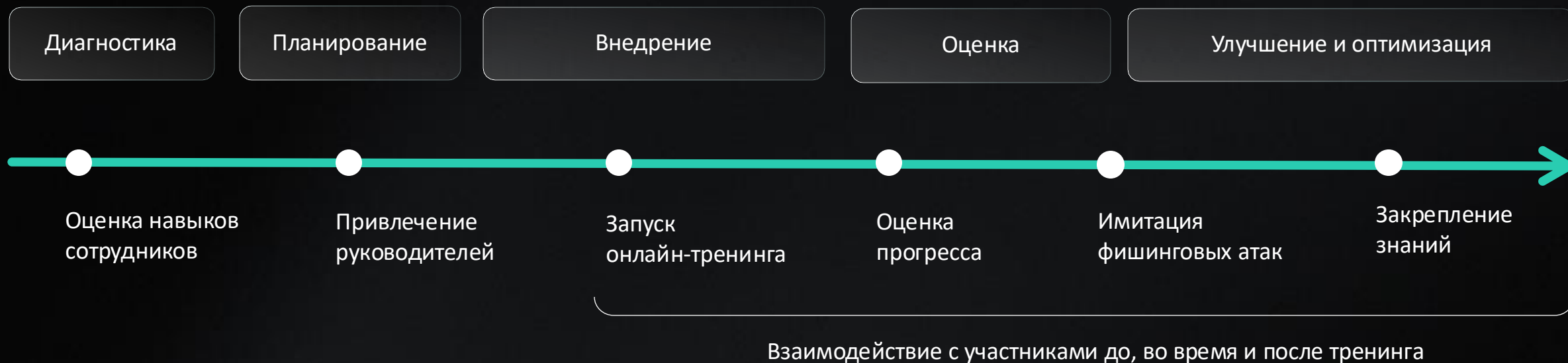
Из чего складывается культура киберграмотности?

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

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



Формирование культуры, ориентированной на безопасность



Инструменты



Kaspersky Automated
Security Awareness
Platform



Kaspersky Cybersecurity
for IT Online



Kaspersky Interactive
Protection Simulation



Kaspersky
Executive
Training

Шаг 1. Имитация фишинговой атаки для оценки текущих навыков сотрудников в сфере кибербезопасности

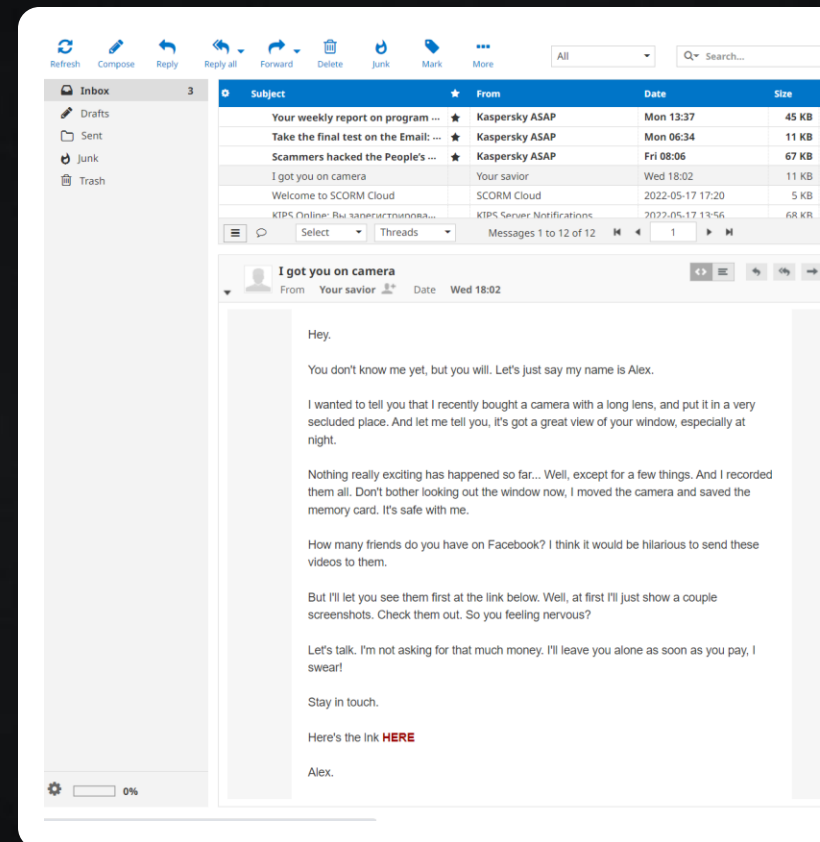
Реализация

Определите исходный уровень уязвимости сотрудников.

Представьте руководству обоснование необходимости тренинга.

Распределите сотрудников по группам.

Назначьте программу обучения каждой группе.



Шаг 2. Вовлечение и мотивация ответственных лиц

Реализация



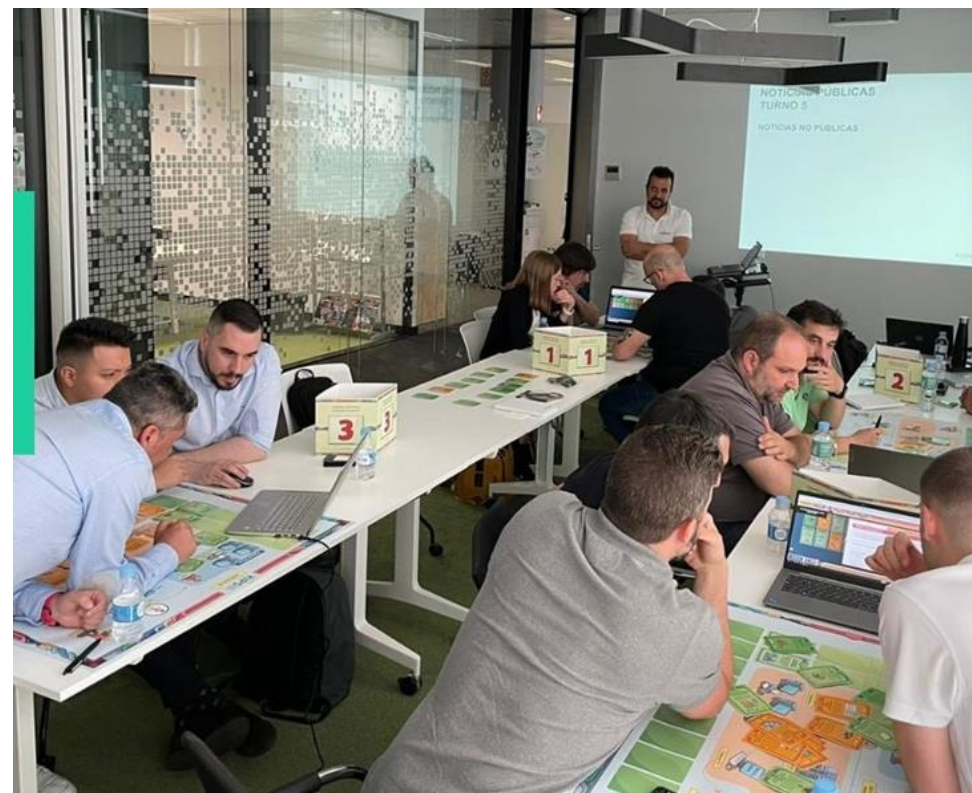
Командная игра KIPS

научит участников защищать финансы компании и повысит мотивацию к обучению.



Kaspersky Executive Training

поможет оценить влияние киберрисков на эффективность бизнеса и освоить способы управления ими.



Шаг 3. Информирование о тренинге и его запуск

Реализация

Поручите специалистам по кадрам и внутренним коммуникациям задачу информировать сотрудников о проведении тренинга.

Назначьте участникам уроки в соответствии с целью тренинга и ролью сотрудника.

Научите сотрудников распознавать признаки атаки и принимать соответствующие меры реагирования.

Примеры изучаемых тем

Пароли и учетные записи

Электронная почта

Веб-сайты и интернет

Мобильные устройства

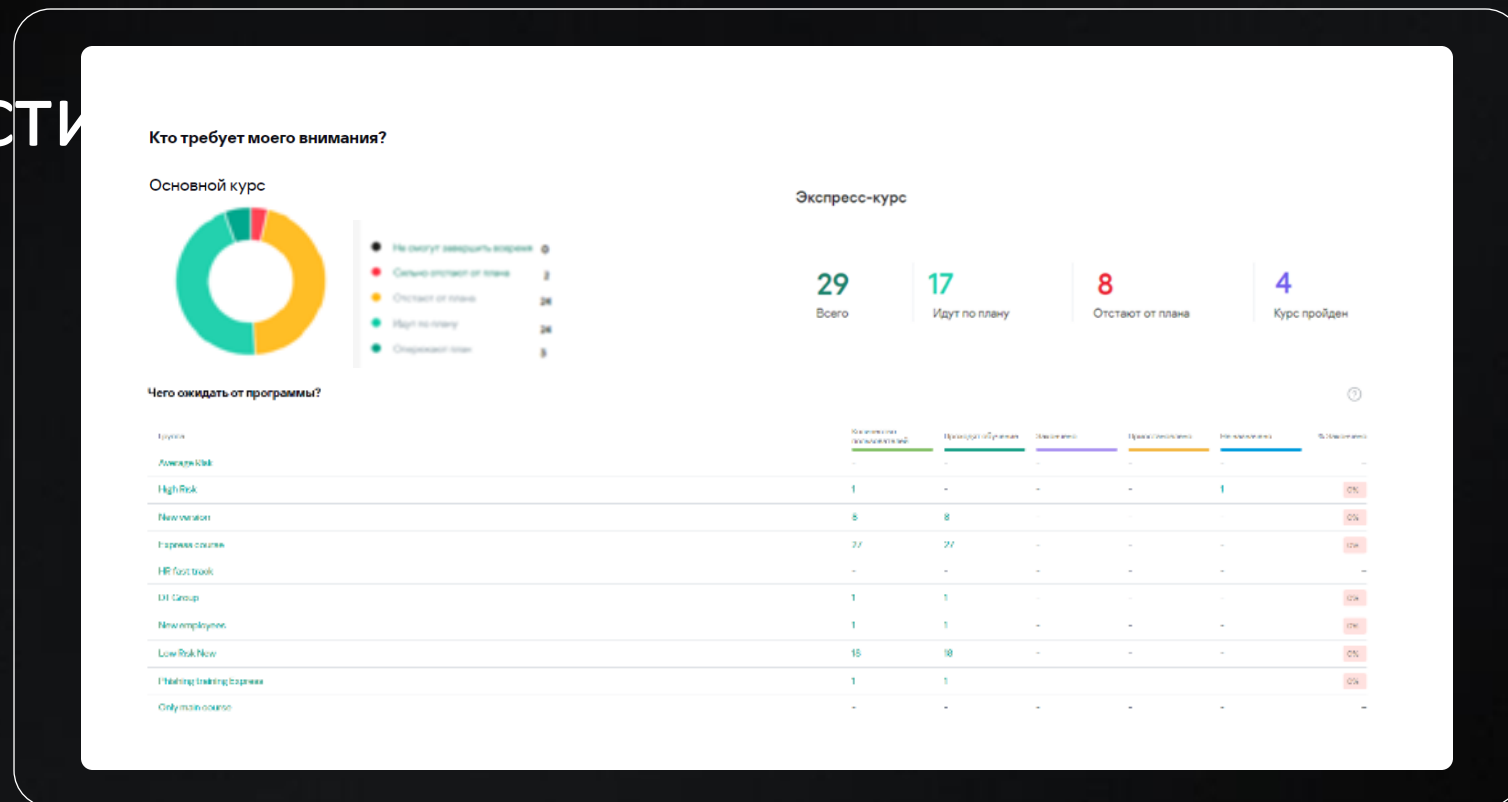
Социальные сети и мессенджеры

Вишинг: борьба с телефонными мошенниками

Искусственный интеллект и нейросети

Шаг 4.

Оценка эффективности



Реализация

Генерируйте отчеты, чтобы оценивать результаты и выявлять проблемы.

Назначайте задания для закрепления материала и проводите фишинговые атаки на основе полученных данных.

Шаг 5.

Имитация правдоподобных фишинговых атак

Реализация

Формируйте нужные модели поведения пользователей, показывая, что опасность может быть совсем рядом.

Назначайте темы с более сложными техниками атак для повышения уровня компетенций сотрудников.

Отслеживайте изменения в поведении.



Bonus calculation for 2025

Your bonus schedule for 2025 has passed financial controls and has been approved. To view your bonus schedule, follow the instructions below.

Please scan the QR code with your smartphone's camera for quick access to your data.



Шаг 6. Закрепление полученных знаний

- Используйте дополнительные материалы:

Баннеры с советами по безопасности

Заставки экрана на ПК сотрудников

Комиксы, мотивирующие безопасное поведение

Поощрения для самых бдительных кибергероев

- Развивайте культуру кибербезопасности, отмечая и поощряя правильные действия сотрудников из разных подразделений.



Эффективный подход к снижению рисков, связанных с поведением пользователей



**Kaspersky
Security
Awareness**



30 лет опыта и экспертизы в области кибербезопасности



Обучение, которое меняет поведение сотрудников на всех уровнях организации

Снижайте число инцидентов безопасности, связанных с человеческим фактором.

Минимизируйте юридические и репутационные риски.

Сокращайте время на управление процессом повышения осведомленности и снижайте нагрузку на IT-специалистов.

Сокращайте возможности наложения штрафов из-за несоблюдения требований.

Ваша
команда-
ваша защита!



Попробовать
бесплатно