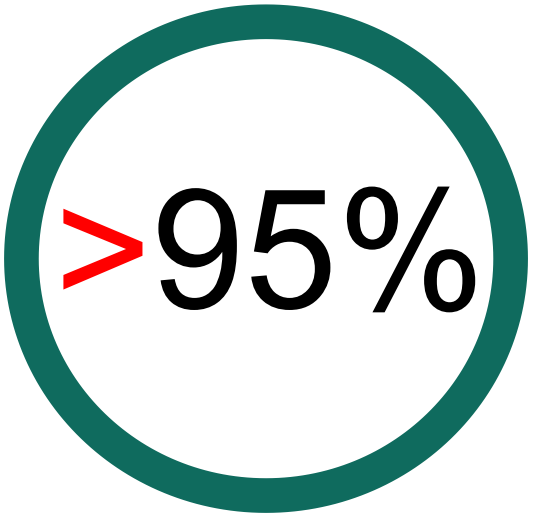
KASPERSKY lab

КИБЕРУЧЕНИЯ.

ГОТОВНОСТЬ НОМЕР 1

Ошибки сотрудников – ключевая угроза безопасности крупных компаний сегодня

Более



Всех киберинцидентов вызваны человеческими ошибками

Только

Страховых программ покрывают случаи, связанные с ошибкой или халатностью сотрудника

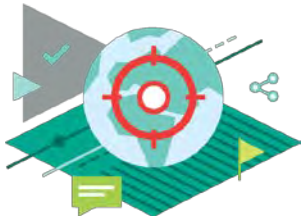
(В то время как риски, связанные с внешними вторжениями злоумышленников, охвачены на 80%)

* IBM 2015 Cyber Security Intelligence Index

2015 Global Cyber Impact Report. Ponemon Institute LLC

KASPERSKY lab

Цена ошибки



$1,155,000

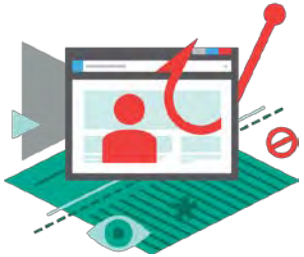
для крупных компаний

$83,000

для компаний
среднего и малого бизнеса

$101,000

для компаний
среднего и малого бизнеса



до $400

на сотрудника в год

* Report: “Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within”, Kaspersky Lab and B2B International, June 2017.

** Calculations based on Ponemon Institute, “Cost of Phishing and Value of Employee Training”, August 2015.

KASPERSKY lab

Подходы к обучению кибер-безопасности

Стандартный подход

- Инструкции, ежегодные презентации, постеры, тренинги

Низкая эффективность
Мало возможностей для измерения результата

Интерактивный подход + инструменты геймификации

- 93% - Вероятность применения полученных знаний в повседневной работе
- 90% - Сокращение числа ошибок
- 50-60% - Снижение рисков кибербезопасности
- Более чем 30 –кратная окупаемость вложений (ROI)

KASPERSKY lab

Проактивный подход

Модель кибер-учений

- Интерактив + замеры ситуации
- Формирование культуры ИБ
- Инструменты геймификации

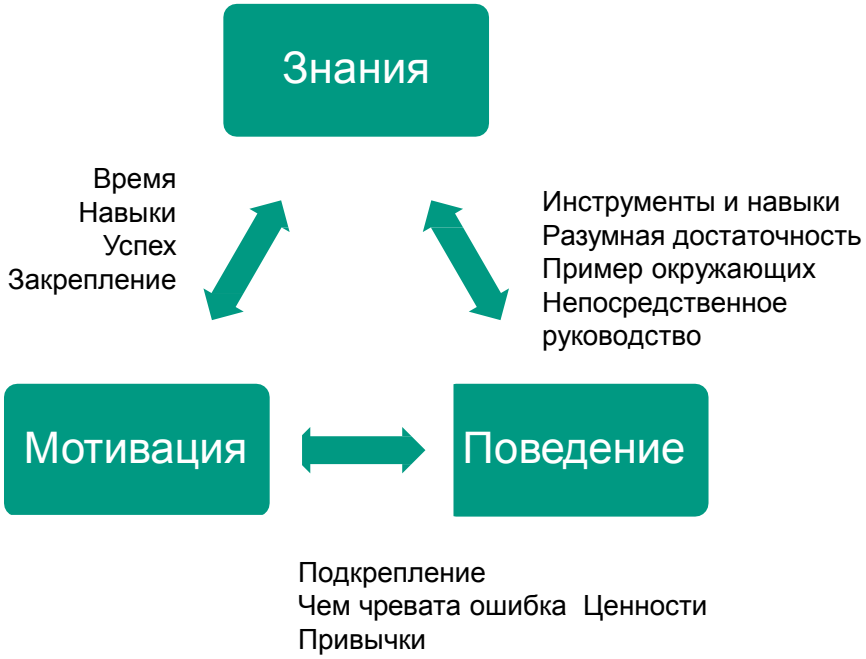
Оценка ИБ-культуры

- Позволяет проанализировать повседневное поведение и их отношение к кибербезопасности

- Онлайн – исследование на основе кратких кастомизированных опросников для сотрудников и менеджеров Развитая система отчетов

KASPERSKY lab

Формирование ИБ-культуры (смена парадигмы)



Большинство программ повышения осведомленности работают только со знаниями.
Но люди устроены иначе: никто не руководствуется только теорией

Поведение – вот с чем надо работать в ходе таких тренингов, а поведение всегда тесно связано с мотивацией и набором знаний.

Предлагаемый нами подход – создание и поддержание культуры кибербезопасности эффективен и измерим на всех уровнях – знания, поведение, мотивации

KASPERSKY

Смена парадигмы (мотивация)

Хакеры сломают мой компьютер	Я не представляю интереса для кибер - преступников	У меня нет времени на безопасность
Опасайтесь людей, а не сломанных компьютеров	Страдают не только те, кто представляет большой интерес	Безопасность необходима для эффективной работы
Подумайте, кто может воспользоваться тем, что вы делаете	Станьте менее уязвимы, чем другие	Сотрудничество с отделом ИБ

KASPERSKY lab

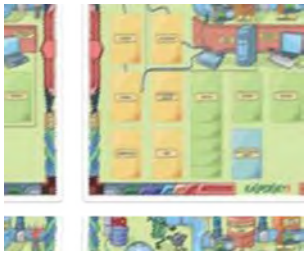
Конечная точка учений

Руководители	Взаимодействие со службой ИБ Понимание ответственности за кибербезопасность
Менеджеры	Формирование безопасной среды в своих подразделениях Упор на более безопасное поведение сотрудников
Все сотрудники	Понимать и разделять ценности безопасного поведения Соблюдать меры кибер-безопасности Сообщать о потенциальных инцидентах

Программы повышения осведомленности

Структура тренингов

Структура тренингов «Лаборатории Касперского» по повышению осведомленности в области кибербезопасности



KASPERSKY lab

KASPERSKY SECURITY AWARENESS (ONLINE)

1 Обучающие модули
29 модулей на все аспекты ИБ

2 Симулированные фишинговые атаки
3 типа атак разной сложности

3 Оценка знаний (assessment) Позволяет настраивать тематику, продолжительность и сложность оценки

4 Аналитика и отчетность позволяет отслеживать уровень обучающихся и динамику изменений

5 Облачная платформа с большим выбором административных ролей
30 языков

KASPERSKY lab

KASPERSKY CYBERSAFETY MANAGEMENT GAMES

- Понимание важности ИБ
- Умение принимать бизнес – решения с учетом принципов ИБ
- Мониторинг
- Убеждение и вдохновение

KASPERSKY lab

KASPERSKY INTERACTIVE PROTECTION SIMULATION

Сценарии:

Bank
Corporation

Oil & Gas

E-Government

Transportation
Power station + Water plant

- Атмосфера соревнования
- Разбор ошибок и анализ оптимальных стратегий
- Деловая игра для выработки стратегии реагирования на киберугрозы
- Командная работа для создания навыков сотрудничества

KASPERSKY lab

Цифры

До

90%

Сокращение числа инцидентов

Не менее

50%

Снижение ущерба в денежном выражении

До

93%

Вероятность применения навыков в повседневной работе

Более чем

30x

Окупаемость вложений (ROI)

Факты

- Банк
- Нефтяная компания
- Ритейлер
- Производственная компания
- Оператор связи