



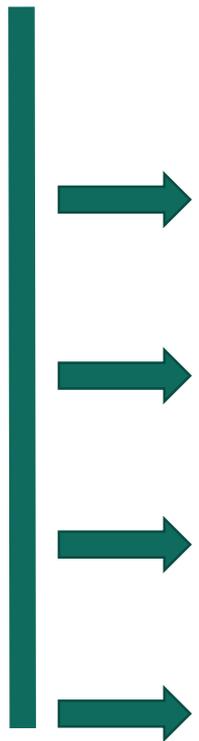
КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Kaspersky Automated Security Awareness Platform (ASAP)

Автоматизированная платформа обучения навыкам кибербезопасности

Алексей Колпаков, ГК Примари
akolpakov@primari.ru



- 
- Внедрение решений по информационной безопасности
 - Подбор, монтаж, и запуск в эксплуатацию оборудования
 - Дистрибуция программного обеспечения
 - Техническая поддержка и ИТ аутсорсинг

Ошибки сотрудников слишком дорого обходятся бизнесу

Потребность в эффективных тренингах по ИБ уже очевидна рынку



14,3 млн р.

для крупных предприятий

Средний ущерб от успешной атаки, в т. ч. вызванной неумышленными ошибками сотрудников *



4,3 млн р.

для сегмента СМБ

Средний ущерб от успешной атаки, в т. ч. вызванной неумышленными ошибками сотрудников *



33%

российских организаций

Хотя бы раз за год столкнулись с инцидентами, связанными с ненадлежащим использованием ИТ-ресурсов сотрудниками *



до \$400

на сотрудника за год

Средние потери компаний от фишинга (без учета прочих векторов атак) **

* Исследование «Информационная безопасность бизнеса», «Лаборатория Касперского», весна 2018.

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

Недостатки традиционных программ обучения сотрудников



Непонятно, как
устанавливать цели и
составлять план
обучения



На управление
обучением тратится
очень много времени



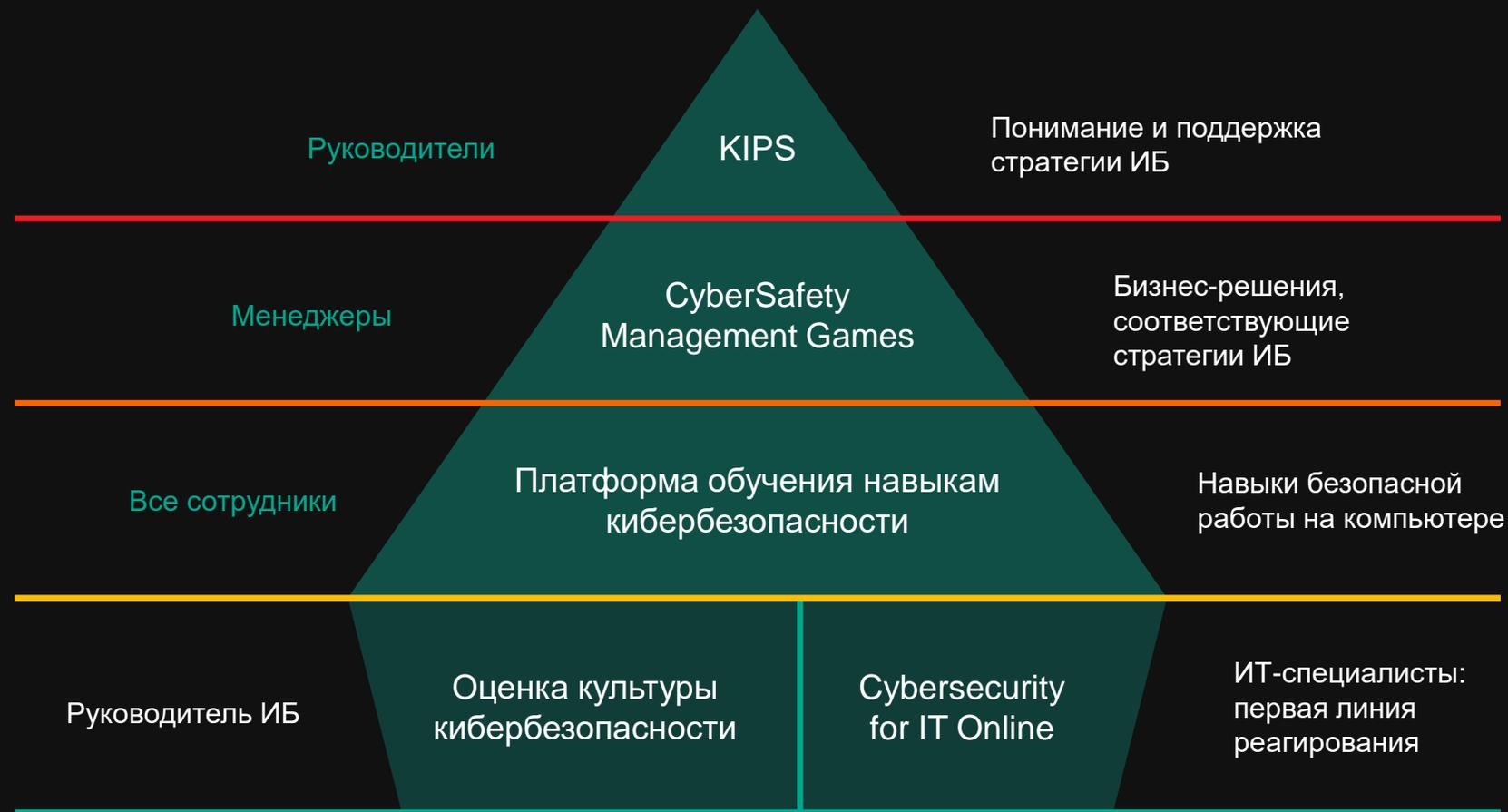
Отчеты не помогают
получить полное
представление о
результатах и
скорректировать
процесс обучения



Ученикам скучно и
неинтересно, поэтому
у них нет мотивации
получать новые
навыки

Все семейство продуктов Kaspersky Security Awareness

Возможность продажи только платформы или целой программы обучения



Реальные навыки, а не просто теоретически знания

«Role-based» тренинги – для всех уровней организации

Компьютеризированные продукты – простота поставки, управления и оценки эффективности

Эффективность за счет геймификации и прикладного характера обучения

Эффективность программ Kaspersky Security Awareness

до

90%

Сокращение
общего количества
инцидентов

не менее

50%

Снижение
финансового
ущерба от
инцидентов

до

93%

Вероятность
применения
полученных
навыков в работе

более чем

30x

Окупаемость
инвестиций в
программы
повышения
осведомленности

рекордные

86%

Участников готовы
рекомендовать
платформу

Kaspersky ASAP – гибкое и простое в использовании решение



KASPERSKY

ПОПРОБОВАТЬ СВЯЗАТЬСЯ С НАМИ RU

01

Kaspersky Automated Security Awareness Training

02

Простой онлайн-инструмент, который поможет вашим сотрудникам овладеть навыками кибербезопасности

03

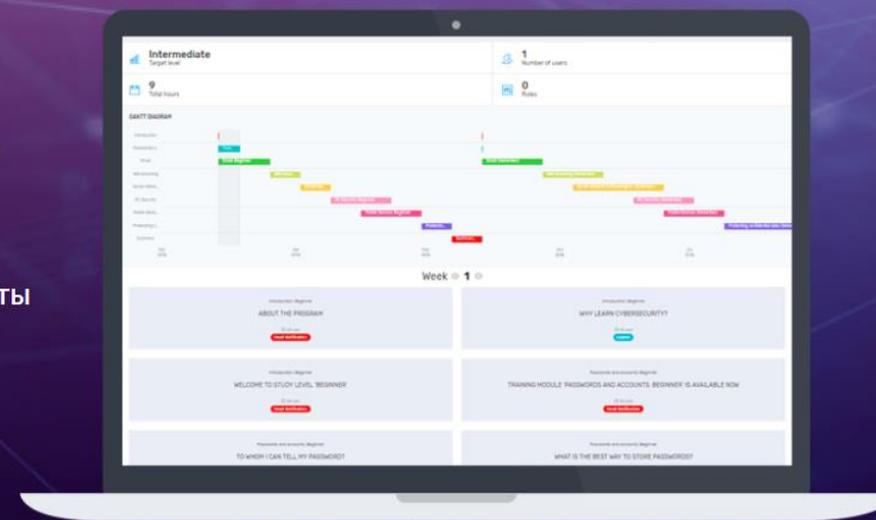
Платформа Kaspersky ASAP создана ведущими специалистами в области кибербезопасности для защиты вашего бизнеса

04

Запустите обучающую программу в несколько кликов

05

ПОПРОБОВАТЬ >



Видео-обзор



Брошюра

Kaspersky Security Awareness: ключевые преимущества



Установка целей и выбор программы

- Установка целей на основе данных «Лаборатории Касперского»
- Возможность сравнения со средними показателями по миру и отрасли



Управление обучением

- Автоматизированное управление
- Построение плана в зависимости от целевого уровня и интенсивности
- Контроль времени обучения



Отчетность и аналитика

- Доступные в любой момент отчеты – действенный инструмент контроля
- Анализ причин невыполнения плана и возможностей улучшения



Удовлетворенность обучением

- Интерактивные упражнения, связанные с повседневными задачами
- Соревновательный подход
- Нет избыточного перенапряжения

1. Установка целей и выбор программы



- Рекомендованный **план обучения** для всех уровней – от базового до продвинутого
- Установка целей **на основе уровня риска и средних показателей** в мире и отрасли
- Простая **оценка и корректировка** хода обучения
- **Экономия времени** – обучение только необходимому
- **Измеримые и видимые** в реальных условиях результаты

Целевые уровни в зависимости от должности сотрудника и необходимости защиты от атак определенного типа

Целевой уровень...	...который позволяет успешно справляться с...	... рекомендованный для (примеры)...	... и занимающий:
I – Начальный	Массовыми (дешевыми и простыми) атаками	Младших специалистов, стажеров	240 минут в течение 2-4 месяцев
II – Базовый	Массовыми атаками на пользователей с определенным профилем	Специалистов по маркетингу, инженеров, административных работников	560 минут в течение 4-7 месяцев
III – Средний	Хорошо подготовленными атаками на выбранную группу сотрудников	HR, финансовых специалистов	800 минут в течение 8-12 месяцев
IV – Advanced	Целенаправленными атаками	IT-специалистов, руководителей организации	1000 минут в течение 10-14 месяцев

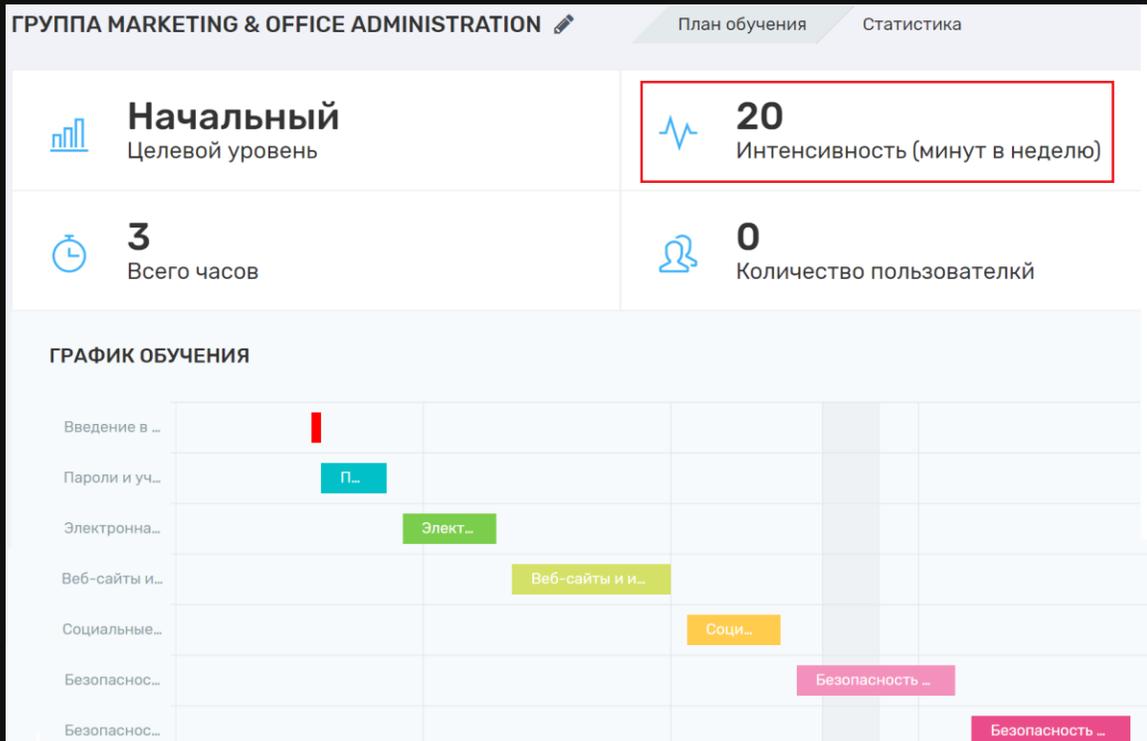
2. Управление обучением



- **Автоматизированное** управление обучением
- **Обширная библиотека** обучающих материалов
- **Мини-уроки в удобном** темпе, которые способствуют получению новых навыков
- Разнообразные **форматы обучающих материалов**
- **Целевой уровень обучения**, зависящий от уровня риска, который представляет сотрудник, определяет количество необходимых уроков

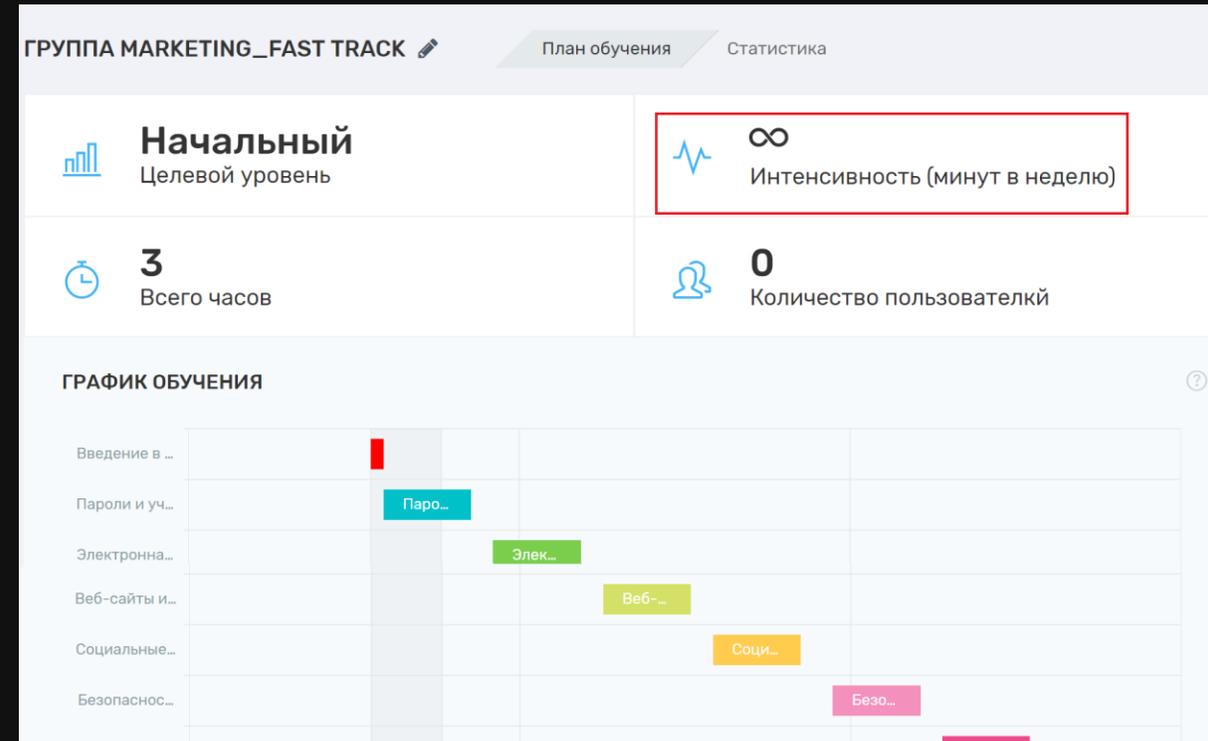


Kaspersky ASAP автоматически строит расписание в зависимости от требуемого уровня и темпа обучения



Обучение длится 15 недель

Средняя продолжительность изучения 1 темы – 17 дней



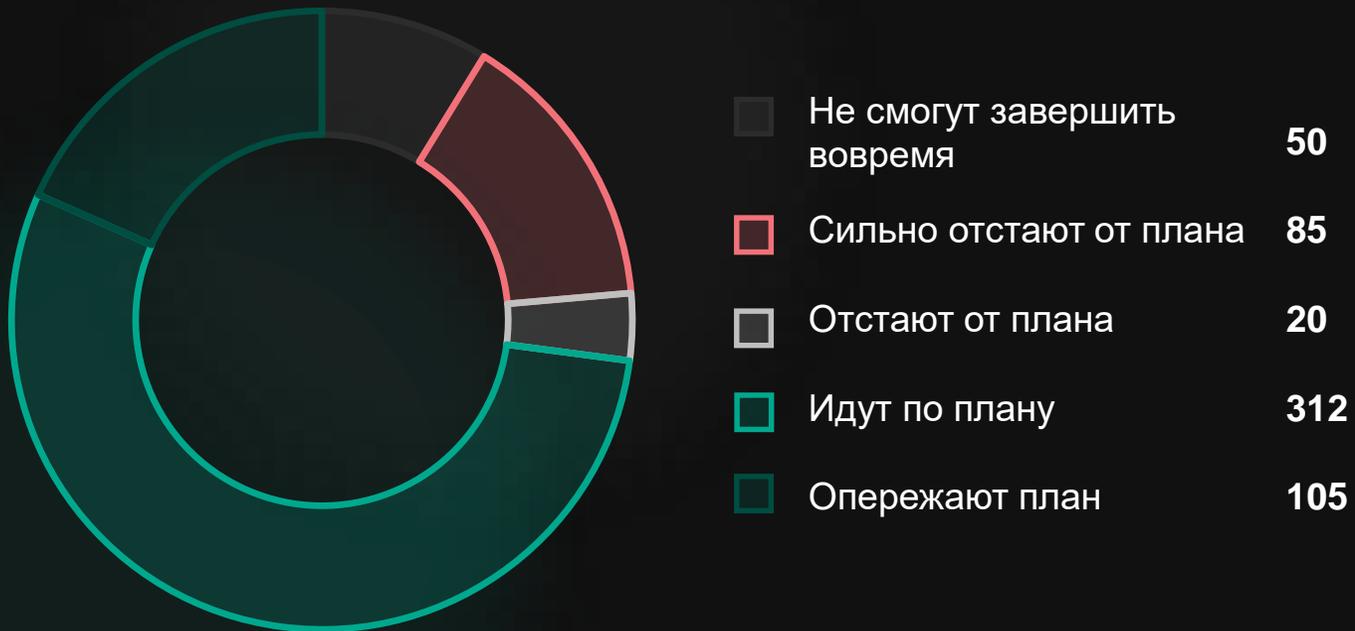
Обучение длится 10 недель

Средняя продолжительность изучения 1 темы – 8 дней

3. Отчеты и аналитика



Чему уделить внимание?

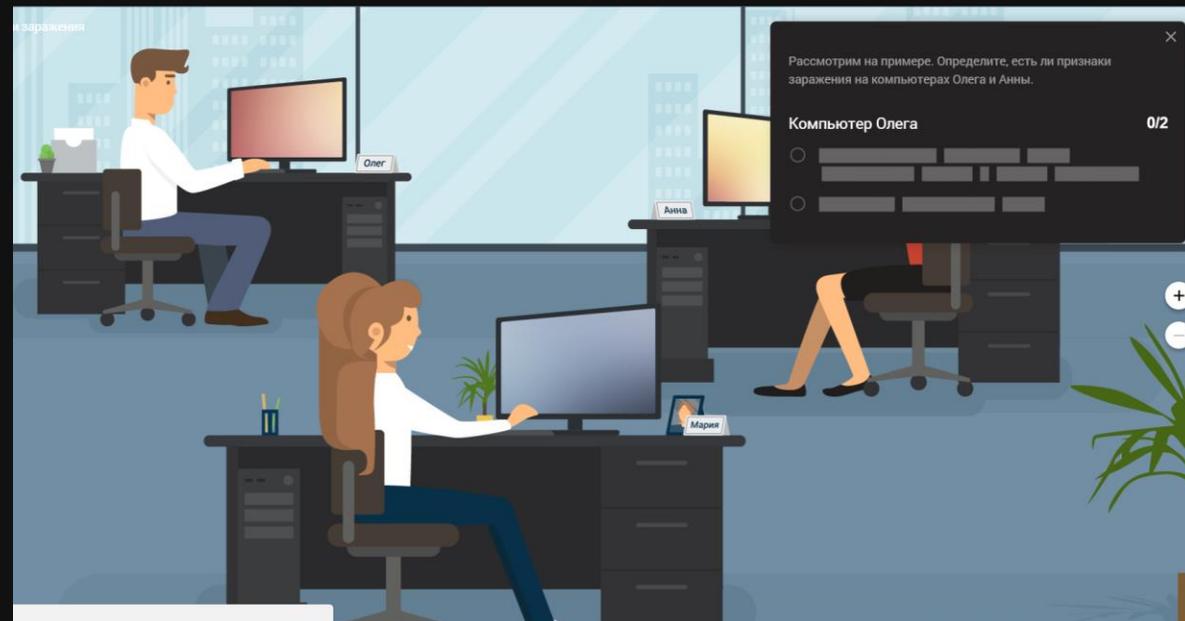


- Применимые на практике **отчеты**
- **Статистика** – по организации, отделу, месту, рабочим обязанностям, а также на индивидуальном уровне
- **Мониторинг** уровня знаний сотрудников и динамики их обучения
- **Анализ «на лету»** помогает понять, что и где можно улучшить
- Удобное сравнение со **средними показателями по миру/отрасли**

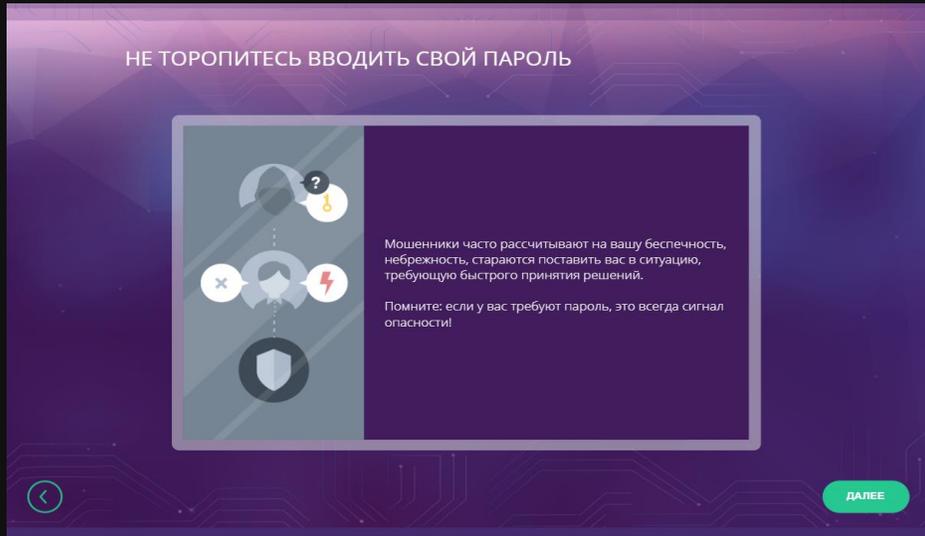
4. Удовлетворенность обучением



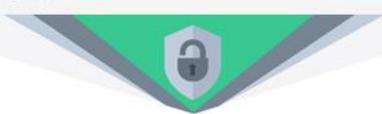
- **Настоящая геймификация** – учиться кибербезопасности интересно!
- **Мотивация** благодаря соревновательному духу
- **Темы, которые часто встречаются** на практике в корпоративной среде
- **Никакой излишней нагрузки** – микроуроки, удобный темп обучения и только нужные навыки



Практичные и интересные микроуроки: Мотивация + теория + закрепление навыка + тест + симулятор фишинга



Тема письма: Правильное хранение паролей – одно из важнейших условий информационной безопасности.
От кого: ASAP
Кому: vasia@rogaikopyta.ru



Правильное хранение паролей – одно из важнейших условий информационной безопасности.



Здравствуйте, Василий!

Зачастую пароль – единственное, что стоит между нашей информацией и злоумышленниками.

Из-за неправильного хранения паролей может пострадать кто угодно



13 января 2018 года жители Гавайев [получили](https://tioumal.ru/65054-otravivshava-lozhnoe) ложное оповещение о запуске по островам баллистической ракеты, ошибочно отправленное сотрудником агентства штата по чрезвычайным ситуациям. Через несколько дней пользователи социальных сетей [нашли](https://tioumal.ru/65054-otravivshava-lozhnoe) старую фотографию из штаб-квартиры того же агентства, где можно увидеть стикер с паролем: <https://tioumal.ru/65054-otravivshava-lozhnoe>

Создавайте сложные пароли, отдельные для каждого ресурса, и никому не предоставляйте к ним доступа.

Любые вопросы о программе задавайте по адресу: support@rogaikopyta.ru

Будьте начеку!
Служба поддержки ООО "РиК"



ТЕМА: ПРОСМОТР ВЕБ-САЙТОВ

Что делать, если поисковый сервис, браузер или антивирус считают сайт опасным?

НАЧАТЬ УРОК

2 ИЗ 17

Выберите правильный ответ и нажмите на кнопку «ОТВЕТИТЬ»

Вам пришло письмо от администраторов сервиса, которым вы пользуетесь, с просьбой сообщить ваш пароль. Следует ли это сделать?

ДАЛЕЕ

входящие

Тема письма: Внимание! Профилактические работы на почтовом сервере!
От кого: Администратор info@corp-email.info
Кому: vasia@rogaikopyta.ru

Здравствуйте, Пупкин (personal.firstName)!

На нашем почтовом сервере ожидаются профилактические работы. Для обеспечения безопасности всех ваших переписок просим вас ввести пароль от вашей электронной почты в форме ниже и нажать кнопку "Отправить".

В противном случае сохранность содержимого вашего почтового ящика по результатам проведенных работ не гарантируется!

ОТПРАВИТЬ

Администрация почтового сервера

Ключевые возможности Kaspersky ASAP

	KASPERSKY ASAP	ТРАДИЦИОННЫЙ ОНЛАЙН-ТРЕНИНГ
Онлайн-платформа	Да	Да
Симулированные фишинговые атаки	Да	Да
Оценка знаний	Да	Да
Несколько уровней обучения	Да	Нет
Автоматический план обучения	Да	Нет
Полная локализация	Да	Ограничено
Подходит для СМБ (5+ пользователей)	Да	Нет
Подходит для MSP	Да	Нет
Оплата за активных пользователей	Да	Нет
Ежемесячная подписка	Да	Нет

СПАСИБО ЗА ВНИМАНИЕ

Алексей Колпаков, ГК Примари
akolpakov@primari.ru

