

# Kaspersky Automated Security Awareness Platform

---

Защита бизнеса и общества от  
киберугроз, связанных с  
человеческими ошибками

**kaspersky**

**Обучение  
кибербезопасности –  
формальность или новый  
тренд?**



---

Человеческий фактор – главная причина киберинцидентов

# Около 80%\* всех киберинцидентов связаны с человеческим фактором

---

Использовать невнимательность, незнание или небрежность пользователей проще и дешевле, чем пытаться обойти продвинутое защитное ПО

\* По результатам анализа отчетов об утечках данных, предоставленных британскому Управлению комиссара по информации (ICO)



## Люди – самое слабое звено в корпоративной кибербезопасности

**52%**

компаний считают, что сотрудники – это самая большая угроза кибербезопасности\*

**60%**

сотрудников хранят конфиденциальные данные на корпоративных устройствах (в том числе финансовую информацию, электронную почту и пр.)\*\*



**30%**

сотрудников признают, что сообщают коллегам учетные данные своего рабочего компьютера\*\*

**90%**

сотрудников склонны переоценивать свои знания основ кибербезопасности\*\*\*

\* По данным исследования *The Cost of a Data Breach (Ущерб от утечки данных)*, проведенного «Лабораторией Касперского» весной 2018 г.

\*\* *Sorting Out Digital Clutter In Business (Наводим порядок в цифровом пространстве)*, «Лаборатория Касперского», 2019 г.

\*\*\*Итоги тренинга «Удаленная работа», «Лаборатория Касперского» & Area9 Lyceum, 2020

# Сотрудники ошибаются, компании теряют деньги

5

Поведение сотрудников остается одним из главных рисков в области ИТ:



**510 000 \$**

(для крупных предприятий)

составляет средний финансовый ущерб киберинцидентов, вызванных неправильным использованием ИТ-ресурсов сотрудниками\*



**465 000 \$**

(для крупных предприятий)

составляет средний финансовый ущерб от утечек данных, вызванный несоблюдением внутренней политики информационной безопасности



**52%**

крупных предприятий

пострадали от киберинцидентов, вызванных неправильным использованием ИТ-ресурсов сотрудниками

(50% малых и средних предприятий)\*\*



более **1,7 млрд \$**

глобальных финансовых убытков

обусловлены компрометацией корпоративной электронной почты\*\*\*

\*Отчет Во что обходятся киберугрозы: рост расходов в сфере информационной безопасности, «Лаборатория Касперского», 2021г.

\*\* Отчет IT security economics in 2019 (Экономика ИТ-безопасности в 2019 г.), «Лаборатория Касперского»

\*\*\* 2019 Internet Crime Report (Отчет об интернет-преступности за 2019 г.), ФБР

В экстраординарной  
ситуации защитят  
самые обычные  
навыки.

Если эти навыки  
есть...



# **Трудности, с которыми сталкиваются компании при организации обучения кибербезопасности**

---

## Болевые точки клиентов



### Сотрудники **не мотивированы** учиться

- Кибербезопасность часто воспринимается как чья-то чужая ответственность
- В среднем более 40% сотрудников не осознают пробелов в своих знаниях, поэтому действуют неправильно будучи уверенными в своей правоте



### **Трудно вовлечь** руководство компании

- 42% руководителей заявили, что ИТ-безопасность не является для них приоритетом
- 58% руководителей высшего звена заявили, что ИТ-безопасность слишком сложна для понимания



## Контент не интересный / не стимулирующий

- Осведомленность о безопасности часто воспринимается как трудная, скучная и рутинная работа
- «Прокликивание» уроков или просмотр видео не способствует изменению поведения



## Полученные навыки не применяются

- Изменение поведения требует от человека отказа от существующей привычки при разработке нового набора действий. Этот процесс требует времени
- Без создания мотивации и повторения 70% изученного забывается в течение одного дня



Как сделать так, чтобы  
сотрудники учились  
тому, что не вызывает у  
них интереса?

Как трансформировать  
знания в действия?  
...причем сделать это  
онлайн

# **Увлекательное обучение кибербезопасности для организаций любого размера**

Эксперты по кибербезопасности знают, что такое безопасное и рискованное поведение

12

В «Лаборатории  
Касперского» знают  
каким должно быть  
**кибербезопасное**  
поведение  
пользователей

Мы переводим наш опыт в  
техники обучения, чтобы помочь  
защитить сотрудников наших  
клиентов от атак



## Комплексное предложение Kaspersky Security Awareness

13

1

### Вовлечение & мотивация

- Интерактивная игра – бизнес стратегия  
**Kaspersky Interactive Protection Simulation**

2

### Определение исходного уровня

- Игровое средство оценки текущего уровня знаний –  
**Gamified Assessment Tool**

3

### Обучение

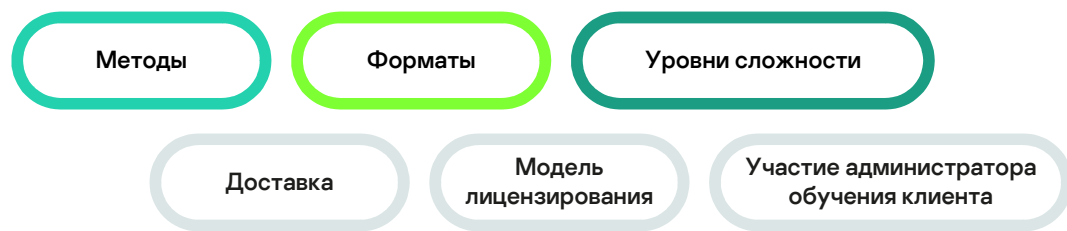
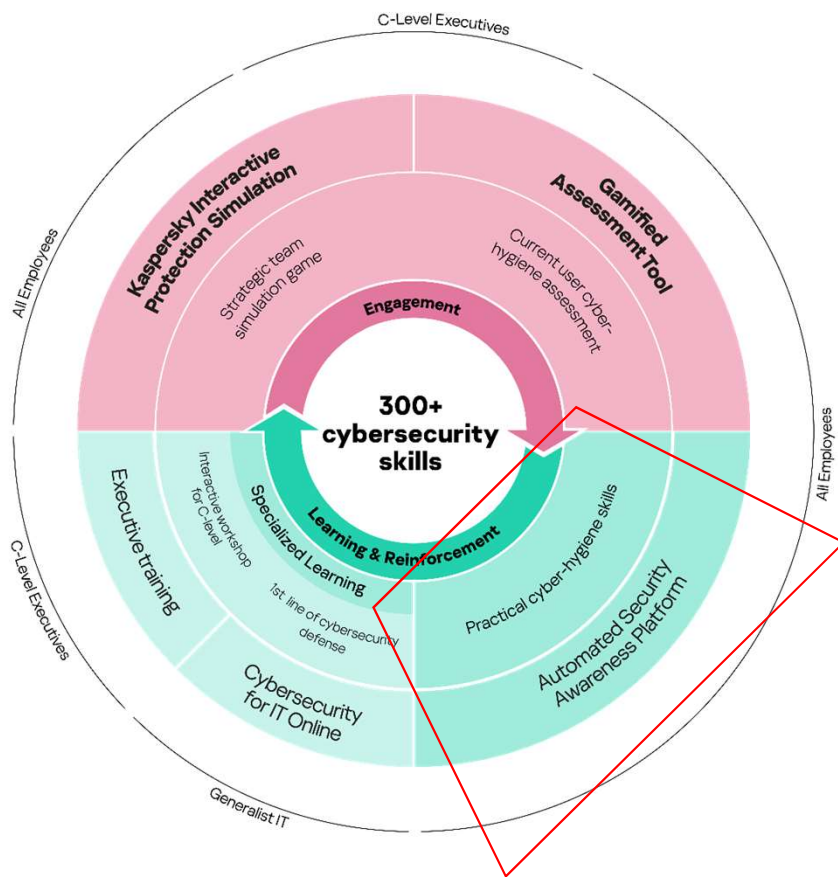
- Обучающая платформа –  
**Automated Security Awareness Platform (ASAP)**
- Онлайн-курс по кибербезопасности для IT-специалистов –  
**Cybersecurity for IT Online**
- Интерактивный воркшоп для руководителей

4

### Закрепление

- Мобильный квест по кибербезопасности  
**[Dis]connected**

# Комплексная программа повышения осведомленности для создания сильной культуры кибербезопасности



# Онлайн платформа Kaspersky ASAP

Учитесь  
Когда и где удобно

15



Kaspersky  
Automated Security  
Awareness Platform



## Kaspersky Automated Security Awareness Platform

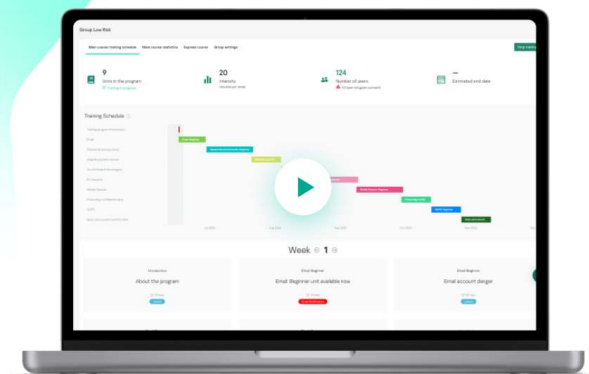
Простой и эффективный онлайн-инструмент, который поможет вашим сотрудникам овладеть навыками кибербезопасного поведения и применять их в работе

Создан ведущими специалистами по кибербезопасности

Купить

Попробовать

Брошюра ▶ Видеообзор



- Эффективность обучения для **СОТРУДНИКОВ**
- Экономия времени на управление программой обучения для **КОМПАНИИ**

[Бесплатный триал](#)



# Содержание курса

План обучения основам кибербезопасности



- Зеленая точка: Электронная почта
- Синяя точка: Пароли и учетные записи
- Светло-зеленая точка: Веб-сайты и Интернет
- Оранжевая точка: Социальные сети и мессенджеры
- Розовая точка: Безопасность ПК
- Красная точка: Безопасность мобильных устройств
- Темно-зеленая точка: Защита конфиденциальных данных
- Синяя точка: GDPR
- Красная точка: Кибербезопасность промышленных систем
- Темно-зеленая точка: Безопасность банковских карт и PCI DSS

## Хэштеги

- #Пароли
- #Фишинг
- #Корпоративные аккаунты
- #Опасные письма
- #Банковские карты
- #Программы-вымогатели
- #Социальная Инженерия
- #Опасные Файлы
- #Работа с браузером
- #Корпоративная этика
- #Антивирус
- #Вредоносное ПО
- #ПриложенияПО
- #Браузер
- #Конфиденциальная информация
- #Хранение информации
- #Передача информации
- #Интернет и Закон
- #Европейское законодательство
- #Бизнес
- #Опасные Ссылки
- #Поддельные сайты
- #Сайты-вымогатели
- #Резервное копирование
- #Мобильные данные
- #Шифрование
- #Облачные сервисы
- #Промышленный шпионаж
- #PCI DSS
- #Двухфакторная аутентификация
- #Цифровой след
- #Торренты
- #Кэтфишинг
- #Целевая атака
- #Персональные данные
- #Хеширование
- #Токены
- #Графические ключи
- #Майнинг
- #Родительский контроль

## Гибкость в отношении объема обучения

Для каждой группы студентов можно выбрать:

- Основной курс или экспресс-курс или их комбинация
- Темы для обучения как на основном курсе, так и на экспресс-курсе

СОДЕРЖАНИЕ

Основной курс Экспресс-курс

**Электронная почта: Экспресс**

- Поиск новых писем и как они работают
- Что делать, если электронную почту взломали
- Как сделать безопасный обмен файлами по почте
- Стоит ли и как стоит отправлять по электронной почте

4 урока, 7 – 10 минут

**Пароли и учетные записи: Экспресс**

- К чему приводит слабое общение с паролем
- Как создать сложный пароль
- Как сделать учетные записи безопасными

3 урока, 10 – 10 минут

**Веб-сайты и Интернет: Экспресс**

- Контент из интернета скрывает угрозы
- Как безопасно загружать программное обеспечение
- Как быть в курсе угроз и фишинга

3 урока, 8 – 10 минут

Основной курс Экспресс-курс

Уровень Начальный

Электронная почта Пароли и учетные записи Веб-сайты и Интернет Социальные сети и мессенджеры Безопасность ПК Безопасность мобильных устройств Защита информации и данных

GDPR Кибербезопасность промышленной системы Безопасность банковских карт и PDI DSS

Содержание

План занятий

Доступные клики

Тесты Сайты, чтобы проверить терпение

Уроки пройдены

Напоминание по почте

Тест

Имитация фишинговой атаки

Модуль пройден

Урок

- Что может угрожать моей электронной почте?
- Что делать, если мою электронную почту взломали?
- На что обращать внимание, если меня просят ввести пароль от электронной почты?
- Какие данные не стоит отправлять по электронной почте?
- Какие электронные письма опасны и как их распознать?

Напоминание по почте

- Мошенники взломали почту Народного банка Китая. А ваша почта в безопасности?

Электронная почта: Начальный

Электронная почта – незаменимый инструмент для любого человека. Даже при наличии корпоративного адреса лично почту продолжают использовать для переписки рабочих документов, общения на рабочие темы, в нерабочее время и для доступа к корпоративным ресурсам, особенно если сотрудники могут работать из дома.

Электронная почта – ключ к множеству других ресурсов. Мошенники понимают это и используют различные способы взломать почтовый ящик, похитить пароль с помощью вредоносного ПО или выманить его у владельца аккаунта. Чтобы понять, насколько распространены эти практики, достаточно знать, что в 2018 году взломали почтовый ящик директора ЦРУ Дюана Бренна.

Что дает компания изучение этой темы вашими сотрудниками?

- Снижение риска взлома почтовых ящиков сотрудников
- Сохранение потенциальных потерь конфиденциальных данных сотрудников
- Уменьшение риска заражения корпоративной сети вредоносным ПО

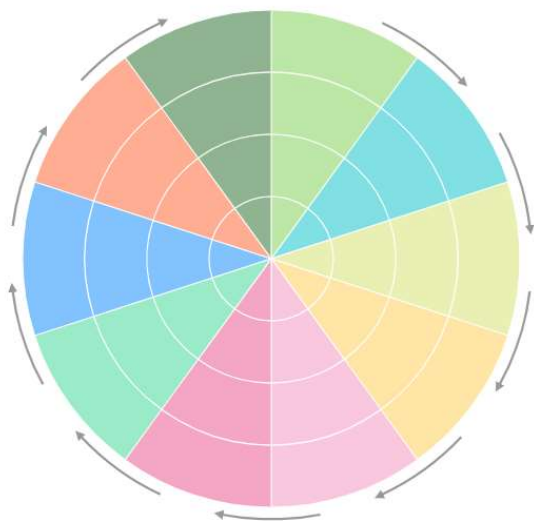
Урок также помогает понять:

- Пароли #Фishing #Опасные письма #Банковские карты
- В учебных активностях, 2–10 мин. каждый

# Платформа Kaspersky Automated Security Awareness Platform: основной курс

## Более 300 конкретных навыков

Универсальный многоуровневый учебный план



- Электронная почта
- Пароли и учетные записи
- Веб-сайты и Интернет
- Социальные сети и мессенджеры
- Безопасность ПК
- Безопасность мобильных устройств
- Защита конфиденциальных данных
- GDPR
- Кибербезопасность промышленных систем
- Безопасность банковских карт и PCI DSS

Учебный план, состоящий из блоков с разными видами активностей для обеспечения максимальной запоминаемости

### План занятий



# Kaspersky Automated Security Awareness Platform основной курс: мультимодальный контент

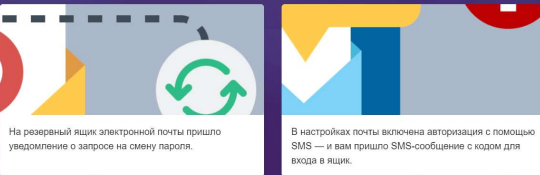
19

# > 200

## ИНТЕРАКТИВНЫХ УРОКОВ

### ПРИЗНАКИ ПОПЫТКИ ВЗЛОМА

А теперь поговорим о том, как распознать взлом. Признаки чужой активности, связанной с вашей электронной почтой, можно поделить на две группы. Первая — это **признаки попытки взлома**. То есть мы еще не знаем, произошел собственно взлом или нет.




На резервный ящик электронной почты пришло уведомление о запросе на смену пароля.

В настройках почты включена авторизация с помощью SMS — и вам пришло SMS-сообщение с кодом для входа в ящик.

НАЗАД ДАЛЬШЕ

### КАК ИЗБЕЖАТЬ ПОТЕНЦИАЛЬНОЙ ОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ BLUETOOTH?

Нажимайте на маркеры списка для получения дополнительной информации



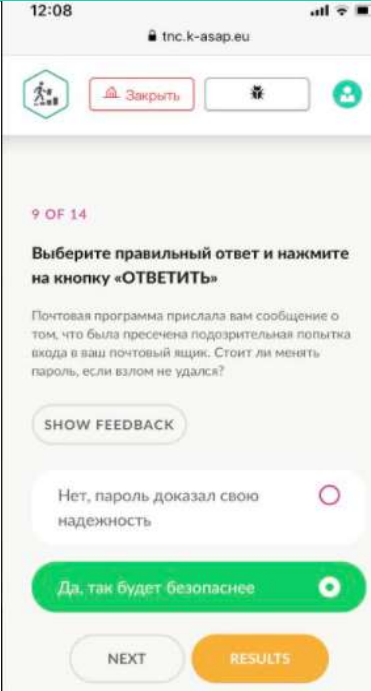
Если ваше устройство постоянно сопряжено с другим (например, с фитнес-браслетом или умными часами), **отключайте режим постоянной видимости Bluetooth**.

Когда вам потребуются, чтобы ваше устройство было обнаружено, включите его специально для этого.



## ТЕСТЫ

12:08 tnc.k-asap.eu



9 OF 14

**Выберите правильный ответ и нажмите на кнопку «ОТВЕТИТЬ»**

Почтовая программа прислала вам сообщение о том, что была пресечена подозрительная попытка входа в ваш почтовый ящик. Стоит ли менять пароль, если взлом не удался?

SHOW FEEDBACK

Нет, пароль доказал свою надежность

Да, так будет безопаснее

NEXT RESULTS




## ЗАКРЕПЛЕНИЕ ЗНАНИЙ


INCOMING

Subject: Property storing your passwords is one of the most important parts of information security.  
From: ASAP  
To: user@(company name).com

You should never use the same passwords for your work and personal accounts



## СИМУЛЯТОР ФИШИНГА



Hello John!

You have registered a new account with Dropbox. If this was you, change your temporary password to a permanent one by following the link:

[Reset your password](#)

If you don't want to change your password, or if this request was made by someone else, immediately go to the [Security Center](#) and cancel the action: scammers could be acting on your behalf.

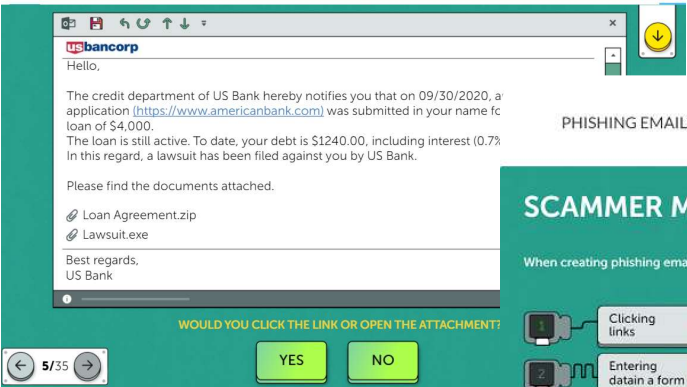
Please do not forward this message to anyone, otherwise your account security could be put at risk. In our help center, you will find [detailed security information](#).

Use with ease!

# Экспресс курс для тех, кто хочет оперативно получить базовые навыки

- Видео
- Короткая интерактивная теоретическая часть
- Тесты & Сертификаты

PHISHING EMAILS AND HOW TO SPOT THEM



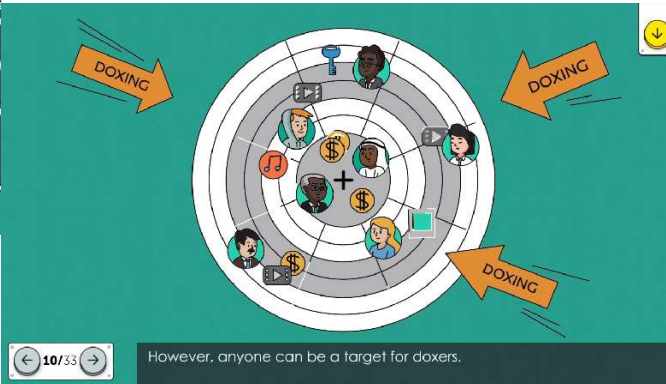
PHISHING EMAILS AND HOW TO SPOT THEM

### SCAMMER METHODS

When creating phishing emails, scammers most often use the following techniques:

- 1 Clicking links
- 2 Entering data in a form
- 3 Downloading attachments
- 4 Social engineering

The link may look 100% reliable, but in fact it is not. For example, you're sent to a fake social site, where you enter your password without noticing anything wrong, thus handing it over to the scammers. Or malware is downloaded that reads data from your keyboard.



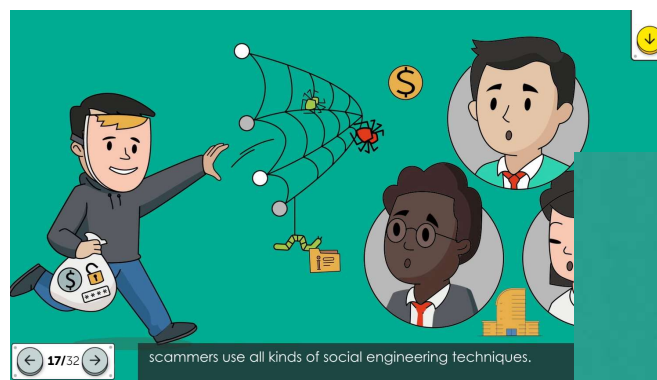
However, anyone can be a target for doxers.

## Экспресс курс, кто хочет оперативно получить базовые навыки

21

### Короткие интерактивные модули по 9 темам:

- Пароли и учетные записи,
- Электронная почта,
- Веб сайты и интернет,
- Социальные сети и мессенджеры,
- Мой компьютер,
- Безопасность мобильных устройств
- Доксинг
- Безопасность криптовалют **НОВАЯ**
- Информационная безопасность при удаленной работе **НОВАЯ**
- Ф3-152 **НОВАЯ**



На данный момент доступно на 8 языках: EN, RU, ES, FR, IT, DE, BR, CN

# Фишинговый симулятор вне пути обучения

22

Проверить устойчивость сотрудников к фишинговым атакам

The screenshot displays the Kaspersky Phishing Simulator dashboard. At the top, the Kaspersky logo and user information (Ekaterina Koshkina) are visible. The main navigation bar includes options like 'Контрольная панель', 'Пользователи', 'Учебные группы', 'Содержание', 'Фишинговый симулятор', and 'Настройка компании'. The 'Фишинговый симулятор' section is active, showing a summary of 7 campaigns with a progress bar and a 'Создать кампанию' button. Below this, a table lists individual campaigns with their names, participant counts, email counts, link clicks, bounce rates, and dates.

Название	Участники	Отправлено писем	Переходы по ссылке	Частота провалов	Начало рассылки	Завершение рассылки	Сбор данных до	Статус
test 1	7	0	0	—	20.12.2020	26.12.2020	02.01.2021	Отменена
Phish Campaign 6	7	7	1	14%	22.10.2020	22.10.2020	25.10.2020	Завершена
Phishing Campaign 5	5	5	4	80%	22.10.2020	22.10.2020	23.10.2020	Завершена
Phish Campaign 4	7	7	0	0%	10.08.2020	14.08.2020	16.08.2020	Завершена
Phish Campaign 3	6	6	0	0%	07.08.2020	07.08.2020	08.08.2020	Завершена
Phish Campaign 2	3	0	0	—	09.08.2020	09.08.2020	12.08.2020	Отменена
Phish Campaign 1	3	3	3	100%	07.08.2020	07.08.2020	08.08.2020	Завершена

- Выбор любой группы пользователей (не связано с назначенным обучением)
- Библиотека готовых шаблонов
- Кастомизация шаблона
- Возможность запланировать фишинговую кампанию
- Отчёт по фишинговой кампании

## Разнообразные фишинговые шаблоны

### Постоянно пополняемая библиотека

Предоставить доступ к таблице?



k.n@support.io **запрашивает доступ** к следующей таблице:

 Publication\_plan.xlsx

**Открыть доступ**

Настройки доступа

Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA  
Вы получили это электронное письмо, поскольку пользователь k.n@support.io запросил доступ к таблице Google.

Google™

Тема: Обновление условий использования  
От кого: Microsoft information@internal-mail.com  
Кому: -



### Соглашение об использовании служб становится более понятным

Здравствуйтесь!

Вы получили это письмо, потому что мы обновляем Соглашение об использовании служб Майкрософт, применимое к продуктам или службам Майкрософт, которыми вы пользуетесь. Мы добавляем пояснения к некоторым положениям, чтобы они были понятны пользователям. Кроме того, обновленное соглашение будет охватывать новые продукты, службы и функции Майкрософт.

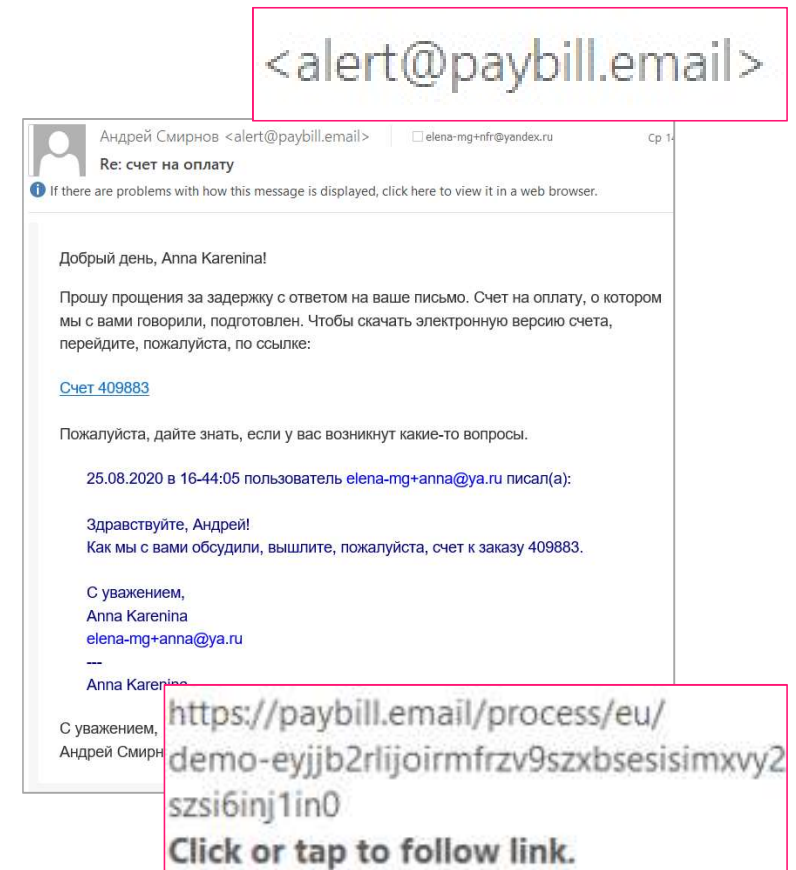
Соглашение об использовании служб Майкрософт — это соглашение между вами и корпорацией Майкрософт (или одним из ее аффилированных лиц), которое регулирует использование веб-продуктов и служб Майкрософт.

Вы можете ознакомиться с Соглашением об использовании служб Майкрософт [здесь](#). Вы также можете узнать больше об этих изменениях на странице с вопросами и ответами [здесь](#), в том числе прочитать краткий обзор самых важных из них. Обновленные условия Соглашения об использовании служб Майкрософт вступят в силу 15 августа 2022 года. Продолжая использовать наши продукты и службы с 15 августа 2022 года, вы принимаете обновленные условия Соглашения об использовании служб Майкрософт.

## Как можно использовать симулированные атаки?

24

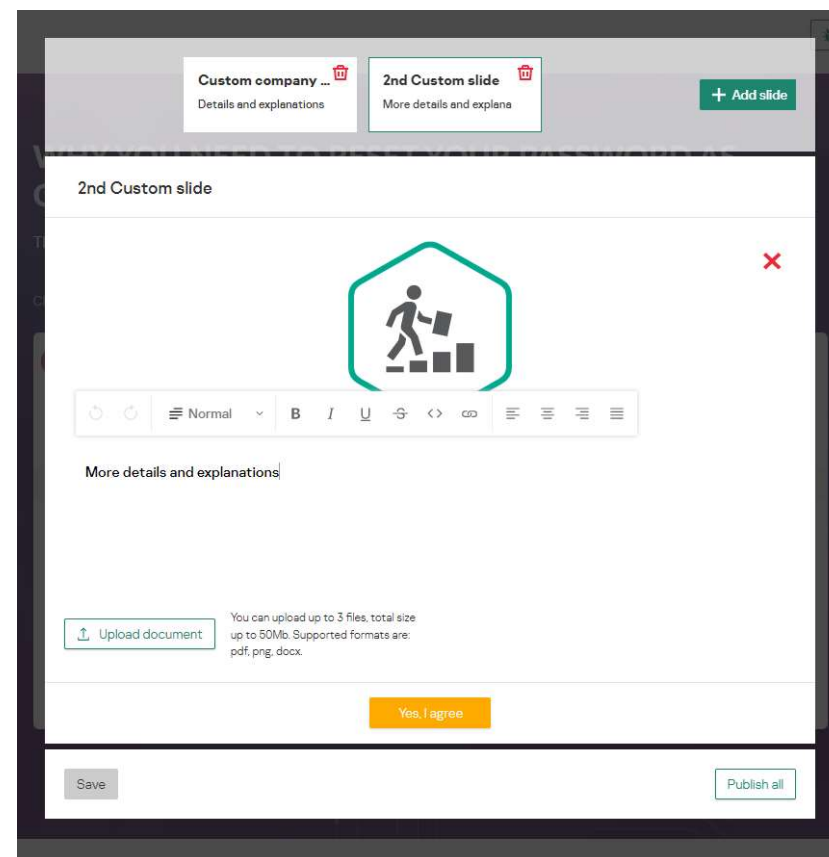
- Определить исходный уровень уязвимости сотрудников,
- Решить, нужны ли компании обучающие курсы для сотрудников, и обосновать решение перед руководством,
- Оценить эффективность обучения (симулированная атака до и после),
- Повысить бдительность сотрудников, показав, что опасность может быть рядом.



Шаблон «Ответ на несуществующее письмо»

# Кастомизация уроков, чтобы соответствовать внутренним политикам и стандартам в организации

- **Добавление необходимой информации**  
Ваши слайды добавляются в любом месте любого урока основного курса
- **Прикрепление файлов в уроках**  
При необходимости загрузите файлы .pdf или .docx с более подробной информацией



# Удобство использования

## Синхронизация с AD Azure

ИМПОРТ И СИНХРОНИЗАЦИЯ

Импорт SCIM

Вы можете автоматически синхронизировать данные о пользователях из Active Directory по протоколу SCIM. Если вы используете Active Directory и SCIM, пожалуйста, обратитесь к администратору AD в вашей компании. Подробную инструкцию вы можете найти [здесь](#).  
После настройки SCIM пользователи ASAP будут автоматически добавляться, изменяться и архивироваться на основе полученной информации. Помните, что процесс синхронизации односторонний и данные, передаваемые из SCIM, имеют более высокий приоритет. Изменения, внесенные в пользовательские данные на платформе вручную, сохраняться не будут.

Тестовый режим ⓘ

URL арендатора (Tenant URL)  История синхронизации

**Обязательные параметры**

Почта

Краткое обращение

Полное обращение

**Дополнительные параметры**

Автоматически применять правила для групп

✕

## ADFS и SSO

НАСТРОЙКА КОМПАНИИ

Общие Пользовательские поля и правила Параметры приветствия SSO

Вы можете настроить доступ пользователей в ASAP с помощью технологии единого входа Single Sign-On (SSO). По умолчанию после создания компании аутентификация с помощью SSO отключена. Пользователи могут переходить на обучающий портал по персональным ссылкам из приглашения на обучение.  
При включении технологии SSO пользователи смогут проходить аутентификацию на обучающем портале с помощью учетной записи провайдера идентификации. Подробную инструкцию вы можете найти [здесь](#).

SAML отключен ⓘ

URL провайдера идентификации\*

Entity ID\*

Сертификат подписи\*  
(PEM в формате X.509)

SSO Sign-in URL  🔗

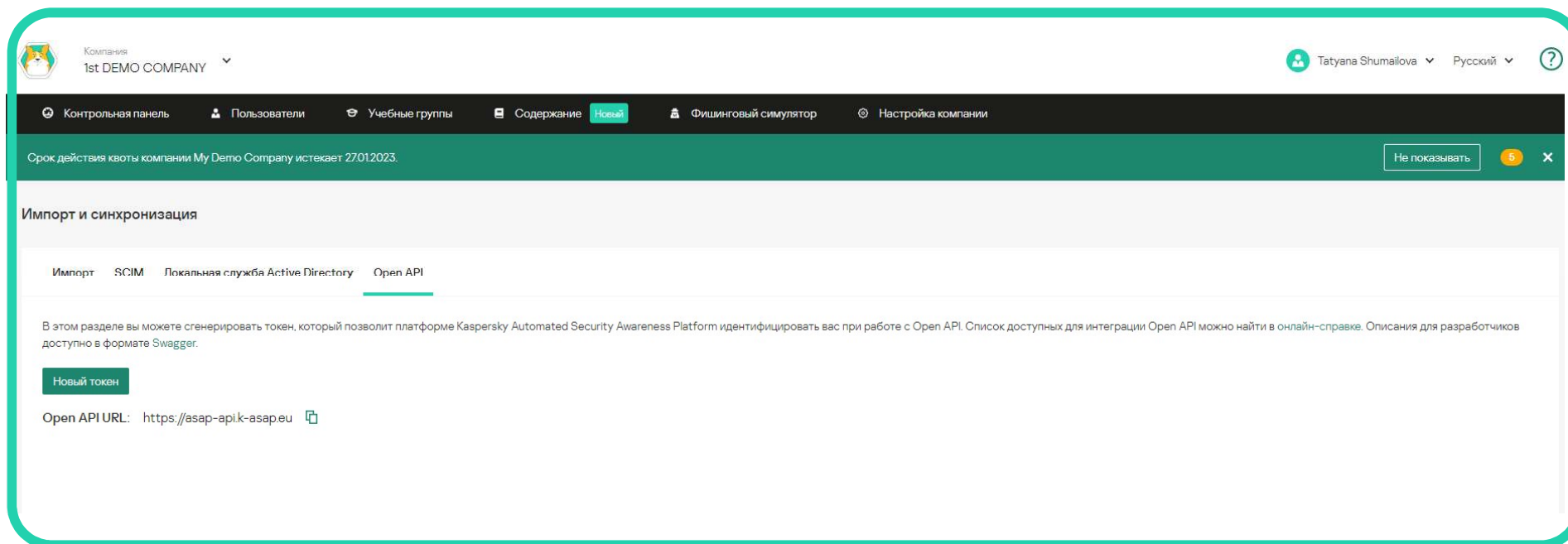
SSO Callback (ACS) URL  🔗

SSO Sign-out URL  🔗

## Удобство использования

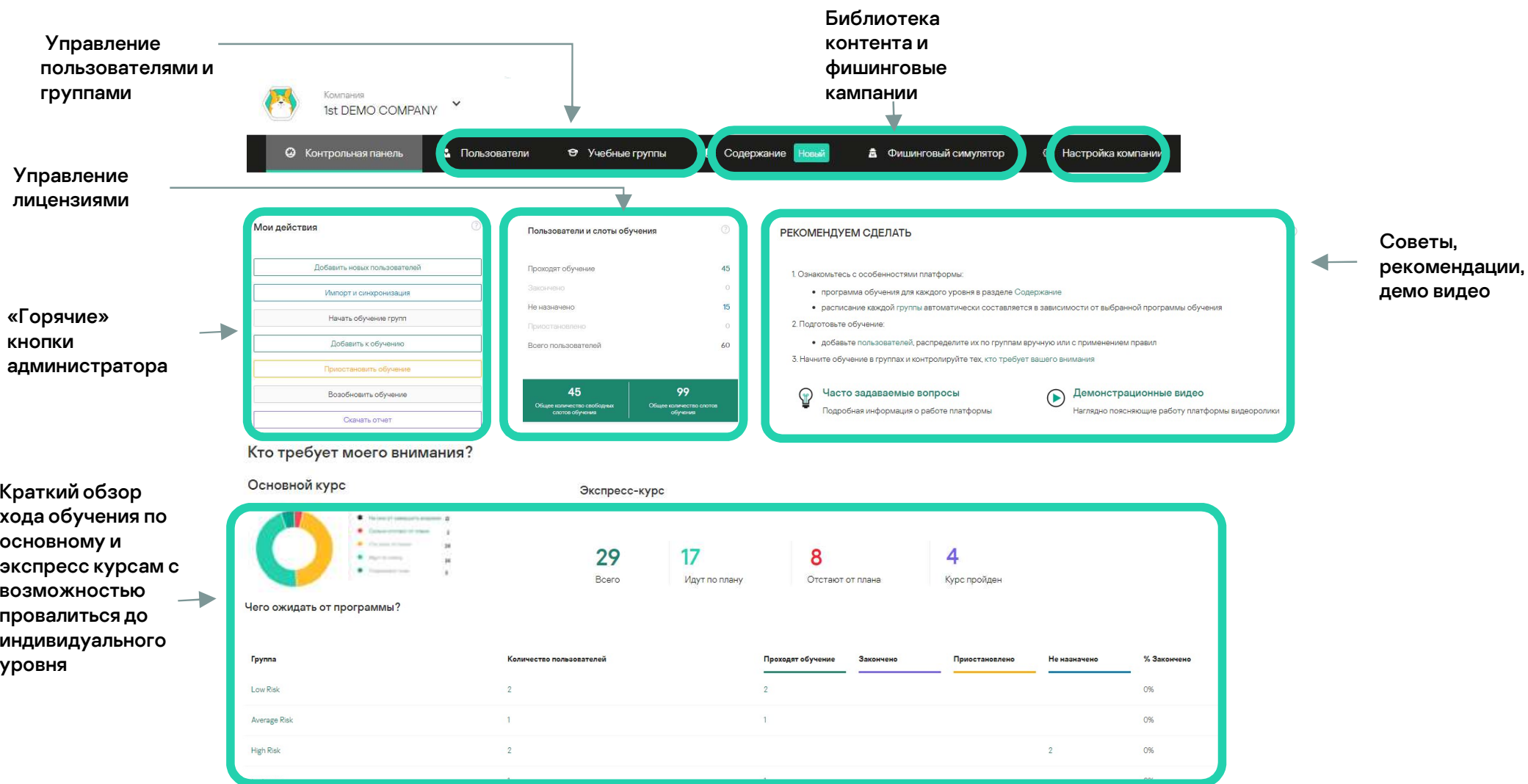
27

### Open OPI – возможность взаимодействия ASAP со сторонними решениями



The screenshot displays the user interface of the Kaspersky ASAP management console. At the top, the company name "1st DEMO COMPANY" is visible. A navigation bar includes options like "Контрольная панель", "Пользователи", "Учебные группы", "Содержание", "Фишинговый симулятор", and "Настройка компании". A notification banner indicates that the company's quota expires on 27.01.2023. The main content area is titled "Импорт и синхронизация" and features tabs for "Импорт", "SCIM", "Локальная служба Active Directory", and "Open API". The "Open API" tab is active, showing instructions on how to generate a token for integration with the Kaspersky Automated Security Awareness Platform. A "Новый токен" button is present, and the Open API URL is listed as <https://asap-api.k-asap.eu>.

# Простой и удобный дэшборд: экономия времени администратора




## Уведомления – элемент внутренних коммуникаций

# Экономия времени на администрирование

### Еженедельные напоминания

Your weekly report on program "The Basics of Cybersecurity"



Greetings, Mofy!

This email contains your weekly report on the training

Planned completion date:  
**05.11.2019**

Estimated completion date: 17.01.2020

**Delay**

In order to study at a comfortable pace and to complete the program on time, we recommend studying regularly, completing incomplete lessons, and proceeding to the next units without waiting for an invitation email.

Below are the recommendations for the modules of the program:

Introduction: Beginner  
Email: Beginner


Expect the email notification about the availability of the test within a few days and immediately take it.

As soon as you catch up, try to keep up with the planned module completion dates and keep studying at the scheduled pace.

[Go to training](#)

### Отчеты администратору

Status: training report on the program "The Basics of Cybersecurity."



Hello, NFR Account!

This email contains a regular report on Status employees' training in the program "The Basics of Cybersecurity". It includes key indicators, a link to the full training report, and a link to recommendations for further work with different employee groups, depending on their current training results.


Key indicators:

Progress	Employees	Recommendation
Ahead of schedule	0	-
Onky well	1	Thank them. See <a href="#">Recommendations</a>
Behind schedule	7	Provide additional motivation to continue training. See <a href="#">Recommendations</a>
Significantly behind schedule	0	-
Can not finish on time	3	Perhaps you need to take advantage of additional organizational measures to engage your employees in training. See <a href="#">Recommendations</a>
total	11	-

[View full training report](#)

### Приглашения

Welcome to the education program



Dear Kitty,

NFR Account ([elena-mg+nfr@yandex.ru](mailto:elena-mg+nfr@yandex.ru)) has added you ([elena-mg+kitty@ya.ru](mailto:elena-mg+kitty@ya.ru)) to the list of students enrolled in the education program "The Basics of Cybersecurity", run by Locomotive.

To start learning, go to your [student portal](#), and confirm your agreement to learn.

We will also ask you to accept the education program privacy policy.

[START LEARNING](#)

If you think you got this message by mistake, please report it to [elena-mg+nfr@yandex.ru](mailto:elena-mg+nfr@yandex.ru).

If you have any questions related to the course, please don't hesitate to ask [elena-mg+nfr@yandex.ru](mailto:elena-mg+nfr@yandex.ru).

Stay Aware!

### Сертификаты

kaspersky

## Certificate

Le présent certificat d'achèvement du module «E-mail : Débutant» confirme que

**Bonaparte Napoleon**

à la suite de sa formation réussie au programme «Les principes fondamentaux de la cybersécurité», est capable de mettre en application des techniques permettant d'utiliser les messageries électroniques personnelles et professionnelles en toute sécurité, notamment en créant des mots de passe complexes et en contrant efficacement la fraude sur Internet.

26/08/2019

Les principes de base de la cybersécurité  
<https://k-asap.eu>

## 4 простых шага, чтобы запустить обучение

30

1

### Загрузить пользователей

Используя AD интеграцию

или

Импортировать из GAT

или

С помощью upload .xlsx файла или

Добавить вручную

2

### Разделить пользователей на группы

Разделить на группы, используя созданные самостоятельно правила

или

Разделить на группы и установить цели обучения на основе ASL

3

### Запустить тренинг

Установить дату начала обучения

4

### Автоматизированное управление обучением, осуществляемое платформой

# On-premise решение

Выпуск: Q4 2023

- Работает даже **без доступа** к интернету
- Развертывание **в сети организации**
- Обеспечивает **высокий уровень конфиденциальности**

---

## Kaspersky Security Awareness: гибкий подход к формированию навыков кибербезопасного поведения 32

**Выберите один тренинг** для решения конкретной задачи безопасности или приобретите пакет технологий, которые можно адаптировать под ваши потребности и приоритеты

### Kaspersky Security Awareness Essential

---

Базовый набор тренингов для повышения осведомленности сотрудников о киберугрозах – простой в установке и управлении

### Kaspersky Security Awareness Advanced

---

Расширенный набор тренингов для более крупных организаций, которым необходимо готовое комплексное решение под ключ.

### Kaspersky Security Awareness Ultimate

---

Максимальный набор тренингов для повышения осведомленности, включающий персонализацию тренингов и доступ к управляемым услугам.

## Пакетные предложения для компаний

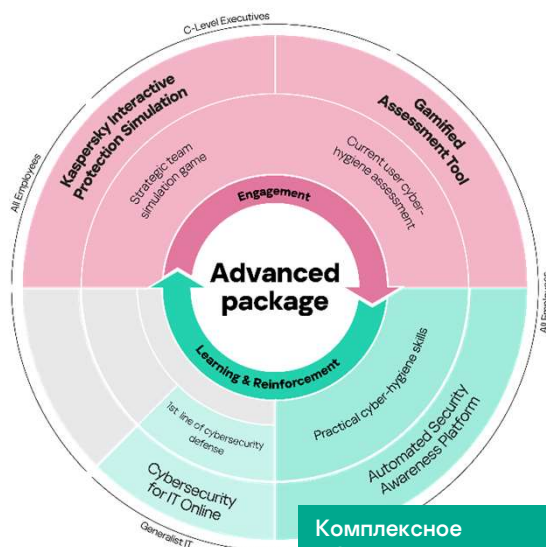
Для среднего размера организаций от 100 пользователей.

Предоставляет стандартный базовый уровень обучения безопасности, чтобы помочь предприятиям успешно работать, защищаться от различных типов атак и соответствовать нормативным требованиям или требованиям третьих сторон по общему обучению кибербезопасности.



Беспроblemный способ повысить осведомленность сотрудников о кибербезопасности — простота настройки, простота управления

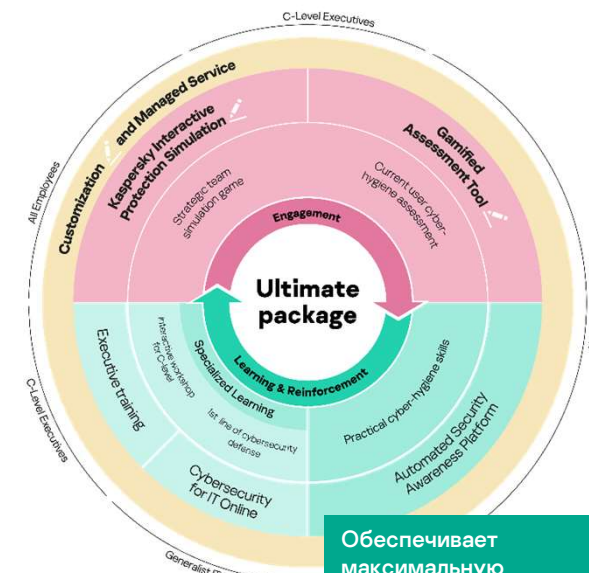
Помогает крупным организациям поддерживать непрерывность бизнеса с помощью простого готового решения для обучения. Включает решения для всех уровней в организации и меняет поведение, охватывая все этапы цикла обучения



Комплексное обучение для крупных организаций, которым требуется готовое решение

Для крупных корпораций, муниципалитетов и пр.

Обеспечивает максимальную готовность к кибербезопасности. Обучение кастомизируется под потребности компании



Обеспечивает максимальную осведомленность о кибербезопасности благодаря кастомизации и управляемым услугам

---

## Пакеты Security Awareness для обеспечения эффективности обучения и увеличение объема сделки

34

Kaspersky Security Awareness

### Essential

“Kaspersky ASAP+”

#### Для кого

Компании, которым необходимо проводить обучение для сотрудников, не связанных с ИТ, но не имеющих опыта обучения и выделенных менеджеров

--

Обычно до 1000 пользователей

Продукты: ASAP, GAT, CITO

#### Ключевое отличие

Тренинг можно развернуть за несколько минут; с автоматизированным обучением и оценкой; простота управления

Kaspersky Security Awareness

### Advanced

“Все продукты”

#### Для кого

Компании, заинтересованные в комплексном обучении для сотрудников всех уровней

--

Обычно 1000+ пользователей, имеющие как минимум 1 специалиста по обучению или выделенный ИТ

Продукты: KIPS, ASAP, GAT, CITO

#### Ключевое отличие

Совместный эффект от разных тренингов продается как одно решение; с геймификацией

Kaspersky Security Awareness

### Ultimate

“Все + кастомизация + сервис”

#### Для кого

Компании, понимающие важность сильной культуры кибербезопасности и желающие адаптировать обучение к своим потребностям

--

Обычно ~ 10,000+ пользователей

Products: KIPS, ASAP, GAT, CITO, Executive Training

#### Ключевое отличие

Программа обучения создана и ведется специально под клиента; с персонализацией и управляемыми услугами

kaspersky

# Будьте в курсе. Защитите себя от кибермошенников

[www.kaspersky.ru/awareness](http://www.kaspersky.ru/awareness)

[awareness@kaspersky.com](mailto:awareness@kaspersky.com)