
KASPERSKY lab
SAVING
THE WORLD
FOR 20 YEARS
ТАЙНЫ ДВОРА
Kaspersky®
Fraud Prevention
Как уберечь данные граждан
от посягательства
Татьяна Пятина
Head of Business Development,
Kaspersky Lab

ЧТО ОБЬЕДИНЯЕТ ЭТИХ ЛЮДЕЙ?

ХРАНИТЕЛИ ДВОРА

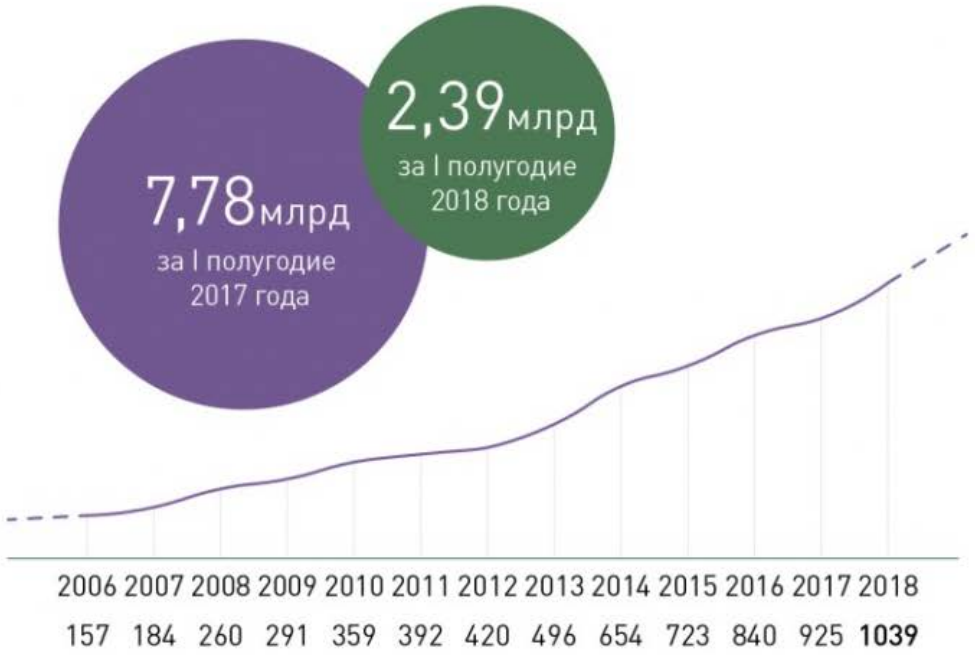
Сэр Томас Кромвель,
1-й граф Эссекс
(правление Генриха VIII)

Кардинал Арман Ришелье
(правление Людовика XIII)

Граф Александр Бенкендорф
(Правление Николая I)

ГЛАВНЫЕ ВЫЗОВЫ

Общее число зарегистрированных утечек информации в I полугодиях 2006-2018 гг.



Распределение утечек по вектору воздействия за I полугодие 2018 года

64,5%
Внутренний нарушитель

35,5%
Внешние атаки

KASPERSKY lab

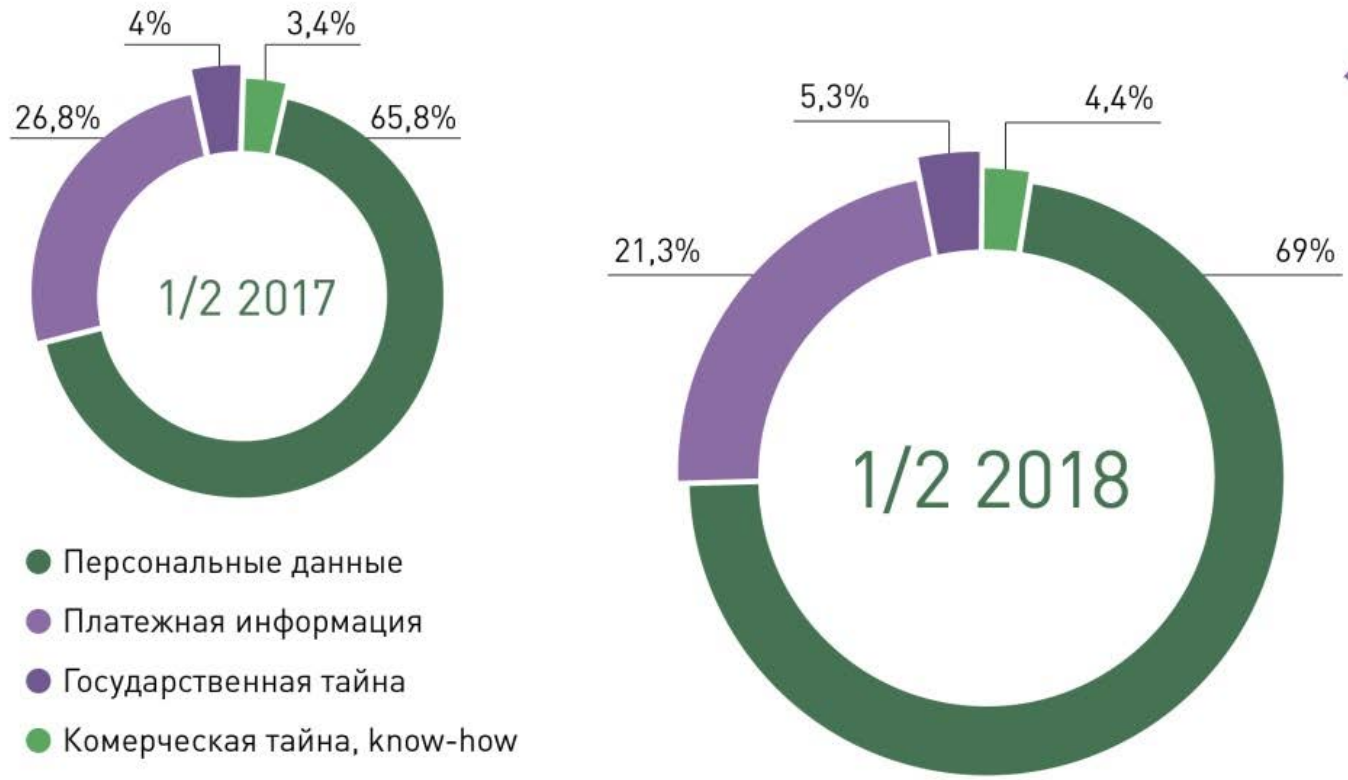
ГЛАВНЫЕ ВЫЗОВЫ

ГЛАВНЫЕ ВЫЗОВЫ

ГЛАВНЫЕ ВЫЗОВЫ

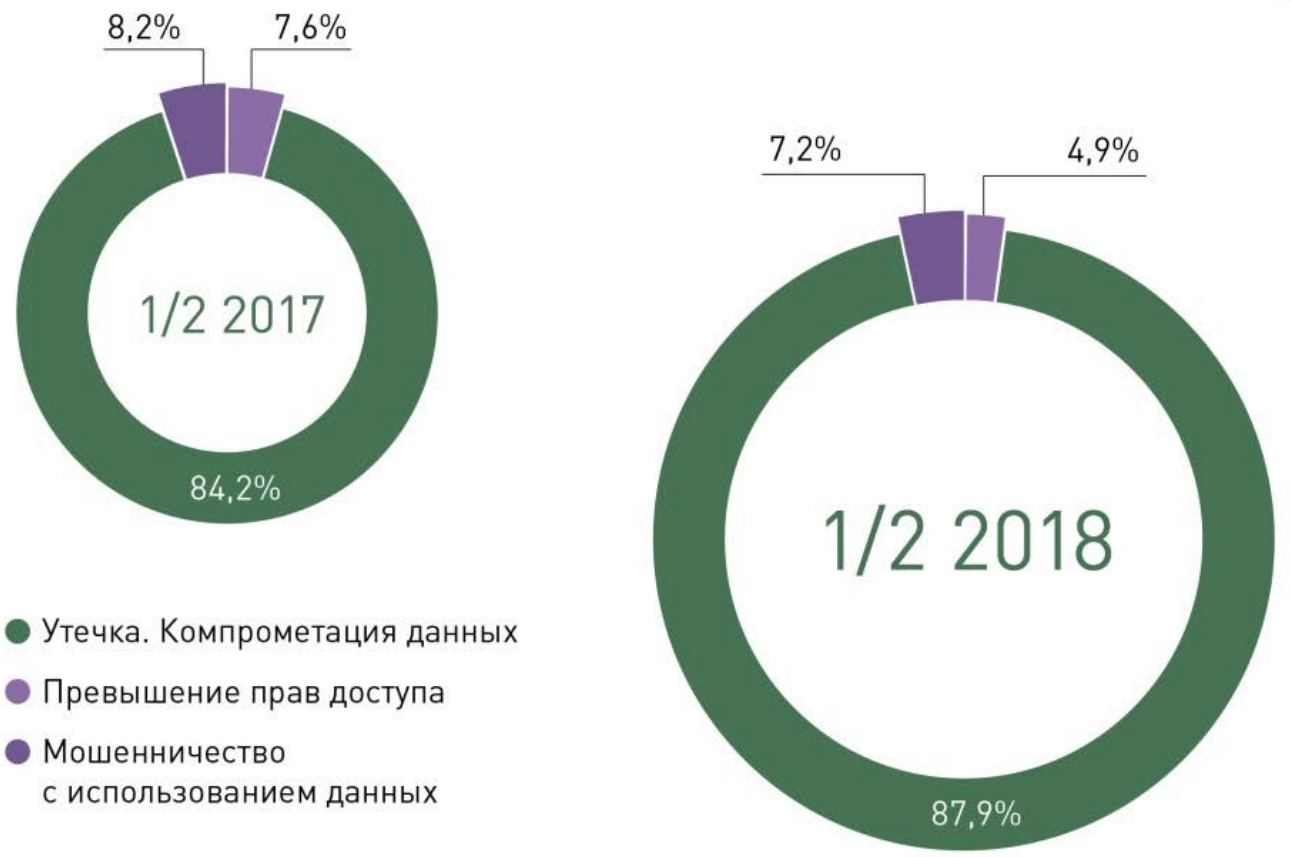
ГЛАВНЫЕ ВЫЗОВЫ

Распределение утечек по типам информации



ГЛАВНЫЕ ВЫЗОВЫ

Распределение утечек по характеру



ГЛАВНЫЕ ВЫЗОВЫ

KASPERSKY lab

ГЛАВНЫЕ ВЫЗОВЫ

Наибольшее количество утечек происходило в высокотехнологичных компаниях (21,3%), медучреждениях (19,5%) и госорганах (13%).

По объему больше всего записей было скомпрометировано в сферах, где чрезвычайно высока ликвидность данных, с которыми работает персонал: в секторе высоких технологий, включая интернет-сервисы и крупные порталы (25,6%), в государственных органах (13%) и муниципальных учреждениях (20%).

ГЛАВНЫЕ ВЫЗОВЫ

- Кража учетных записей или несанкционированный доступ к ним – одна из основных проблем для государственных сервисов
- Текущий подход к аутентификации часто приводит к проблемам с удобством использования
- Устаревшие средства, работающие на уровне транзакции, не могут отличить поведение легитимных пользователей от подозрительного

ПОДХОД

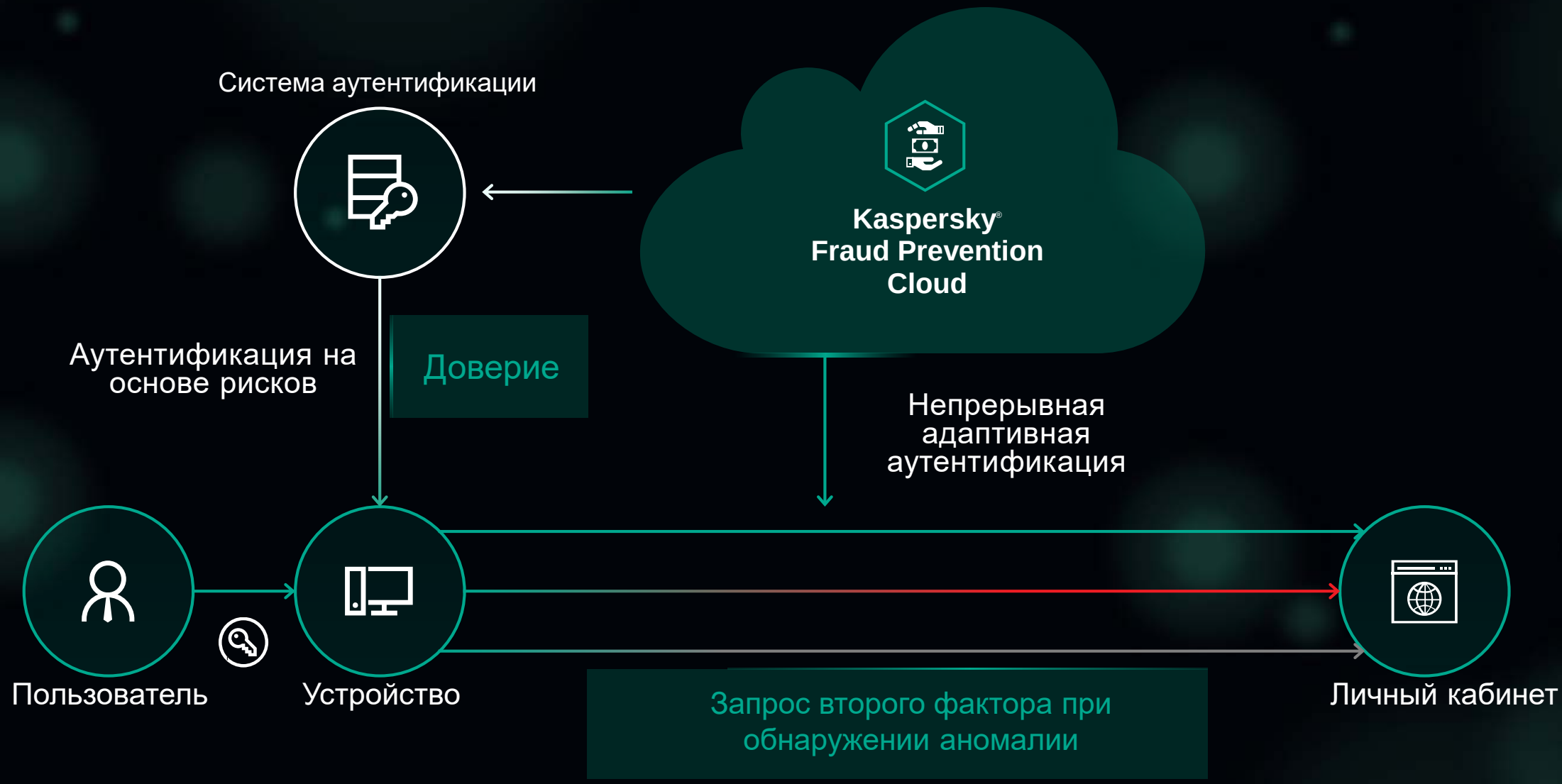
- Внедрение технологий для выявления автоматизированных атак без влияния на клиентов и удобство использования сервисов

- Построение и распознавание шаблонов поведения «хороших» пользователей для сокращения излишних шагов аутентификации

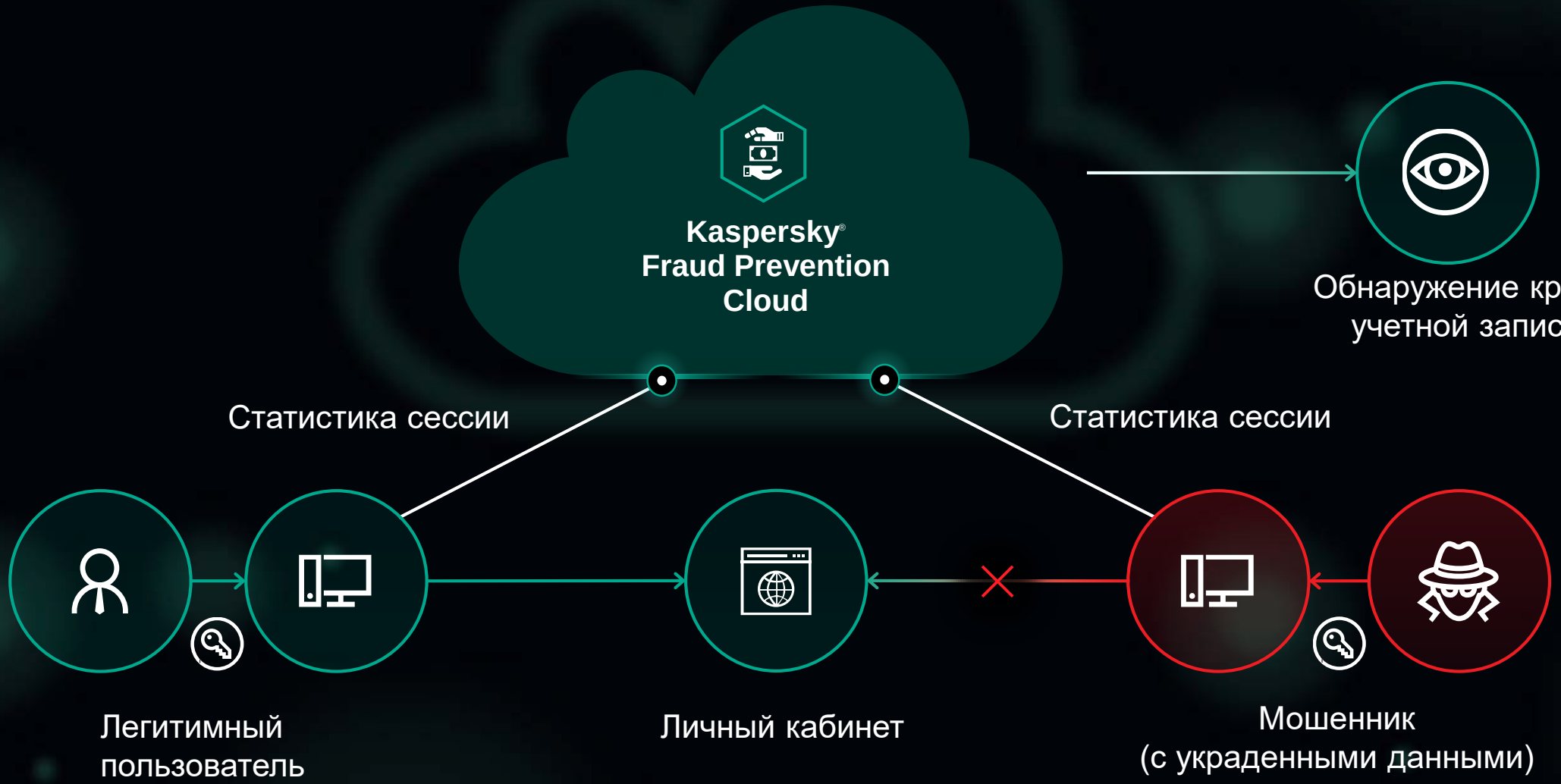
- Применение адаптивного подхода к аутентификации: тщательная верификация при подозрительной активности, беспрепятственный доступ для легитимных пользователей

ADVANCED AUTHENTICATION

СНАЧАЛА ДОВЕРИЕ – ЗАТЕМ НАБЛЮДЕНИЕ ЗА ПОВЕДЕНИЕМ



ОБНАРУЖЕНИЕ КРАЖИ УЧЕТНОЙ ЗАПИСИ



КЛЮЧЕВЫЕ ТЕХНОЛОГИИ

Технология	Описание
Поведенческая биометрия	Построение пользовательских профилей на основании событий мыши, клавиатуры, использования мобильных устройств
Поведенческий анализ	Построение поведенческих шаблонов легитимных пользователей и мошенников
Анализ устройства и окружения	Глобальная репутация «хороших» и «плохих» устройств, основанная на статическом и динамическом отпечатке браузера
Обнаружение вредоносных программ	Обнаружение различных видов вредоносного ПО как в онлайн, так и в мобильном каналах


Kaspersky®
Fraud Prevention
Вопросы?
KASPERSKY lab