Цифровая безопасность

Наша цель — защищать пользователей от киберугроз с помощью продуктов и инициатив «Лаборатории Касперского».

В современном цифровом обществе технологии все глубже проникают в повседневную жизнь людей, и вместе с этим постоянно растет количество киберугроз. В то время, когда вы обмениваетесь сообщениями, скачиваете фотографии или проводите онлайн-операции, вы можете подвергаться опасности. Злоумышленники совершенствуют методы кибератак, вторгаясь в личную жизнь людей. Мы стремимся защитить интересы пользователей в информационном пространстве и сделать его местом, где каждый человек чувствует себя в безопасности.

Решения «Лаборатории Касперского»

>411 тысяч
новых вредоносных файлов обнаруживали ежедневно в 2023 году

33 790 599
атак с использованием вредоносного, рекламного или нежелательного мобильного ПО предотвратили в 2023 году

~125 млн
вредоносных файлов нашли с января по октябрь 2023 года

135 980 457
вредоносных почтовых вложений заблокировали в 2023 году

>437 млн
кибератак отразили с ноября 2022 года по октябрь 2023 года

709 590 011
попыток перехода по фишинговым ссылкам предотвратили в 2023 году

Как мы защищаем пользователей от киберугроз

Чтобы противостоять киберугрозам, мы создаем качественные продукты и ведем просветительскую работу, обучая основам цифровой грамотности пользователей и основам кибербезопасности корпоративных клиентов.

TC-SI-230a.2

Наши решения защищают пользователей от широкого спектра киберугроз: онлайн-мошенничества, утечек данных, целевых кибератак. Чтобы получить контроль над компьютерными системами, злоумышленники используют различные виды программ.

- **Вирусы** — программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы компьютера, они копируют сами себя.
- **Троянцы** — программы, осуществляющие несанкционированные пользователем действия: уничтожают, блокируют, модифицируют или копируют информацию, нарушают работу компьютеров или компьютерных сетей. Одно из ключевых отличий этого класса вредоносного ПО — неспособность к самовоспроизведению. Первые представители появились еще в конце 1980-х годов и полностью соответствовали своему названию, выдавая себя за легитимное ПО.
- **Шпионское ПО** — программы, втайне следящие за действиями пользователя и собирающие информацию, которую злоумышленники используют в своих целях.
- **Шифровальщики** — ПО, которое шифрует файлы и данные на компьютере пользователя, после чего злоумышленники требуют выкуп за восстановление доступа к информации, утверждая, что иначе пользователь потеряет данные. Злоумышленники могут также угрожать выложить скомпрометированные данные в открытый доступ.
- **Рекламное ПО** — программы рекламного характера, которые могут создавать проблемы на устройстве пользователя.
- **Ботнеты** — сети компьютеров, зараженных вредоносным ПО, которые злоумышленники используют в своих целях.

Пользователи и компании также могут стать жертвой фишинга, скама, телефонного мошенничества и DoS-атак.

Современный мир стал свидетелем значительного увеличения числа киберугроз по мере развития цифровых технологий и интернета. С каждым годом количество вредоносных файлов растет: если в 2020 году мы обнаруживали около 360 тысяч новых вредоносных файлов в день, то в 2023 году — уже 411 тысяч, что на 3% больше, чем годом ранее.

Количество вредоносных файлов, обнаруживаемых «Лабораторией Касперского» ежедневно, тысяч штук

Боремся с кибersталкингом

Задача

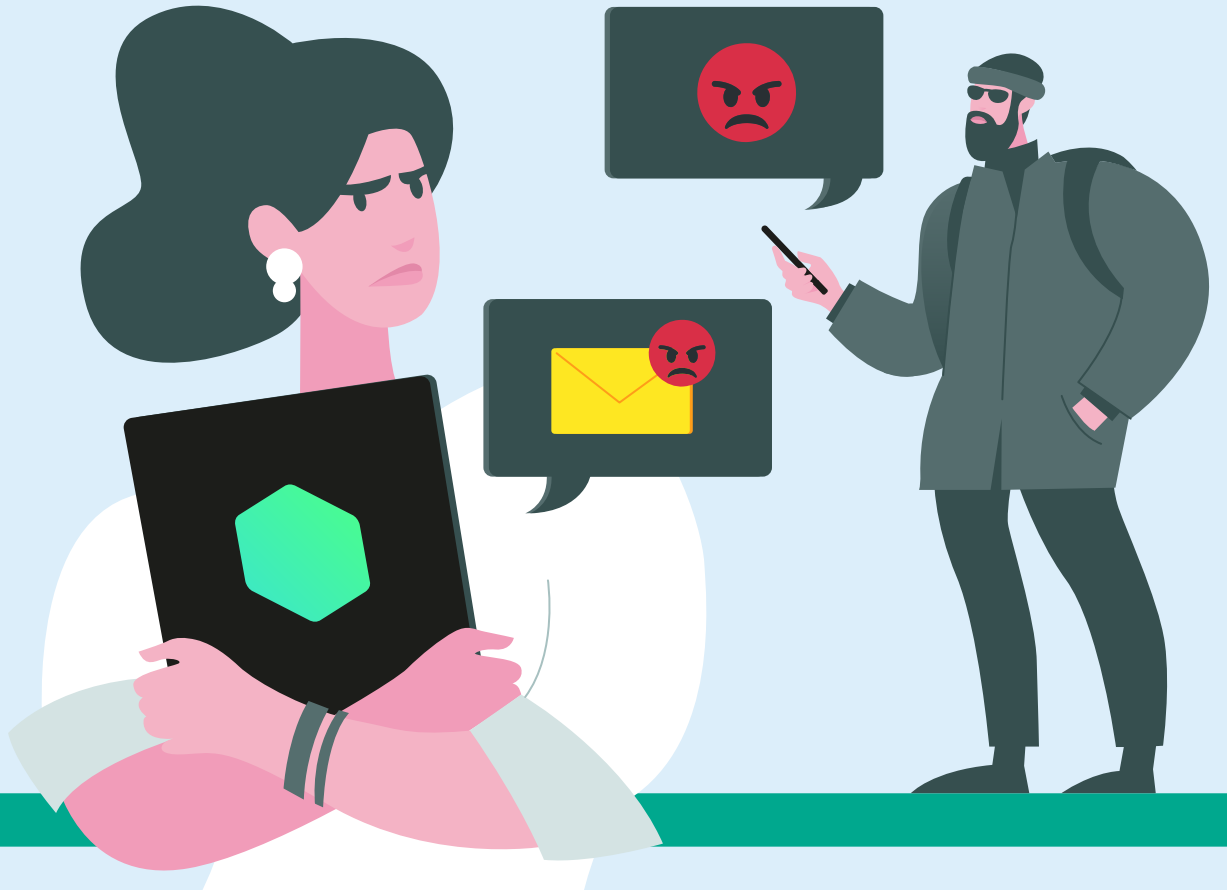
Защита пользователей от цифрового преследования

Результаты наших исследований свидетельствуют об устойчивом росте числа атак с использованием ПО для цифровой слежки, или, иначе, сталкерского ПО. Чаще всего их жертвами становятся жители России, Бразилии и Индии, но в целом это явление распространилось по всему миру.

Сталкерское ПО, или Stalkerware, — это программы, которые используются для скрытого наблюдения за другим человеком (это может быть, например, партнер или член семьи) через его устройство. Это не только техническая, но и социальная проблема, для решения которой необходим вклад всех участников цифрового пространства. Мы уведомляем пользователей об этой угрозе с помощью наших продуктов, в числе которых Kaspersky для Android. Это решение для защиты данных на смартфоне, предупреждающее пользователей в том числе об обнаружении сталкерских приложений на устройстве. Кроме того, мы работаем над решением проблемы кибersталкинга, сотрудничая с некоммерческими организациями, отраслевыми экспертами, исследовательскими компаниями и государственными учреждениями по всему миру и предлагая инструмент для борьбы с цифровой слежкой TinyCheck.

>31 тысячи

пользователей во всем мире столкнулись с кибersталкингом в 2023 году (+5,9% к 2022 году)



Решения

GRI 203-1

Участвуем в проектах по защите от сталкерского ПО

В 2019 году «Лаборатория Касперского» стала сооснователем Коалиции по борьбе со сталкерским ПО (Coalition Against Stalkerware) — международной рабочей группы по борьбе со сталкерскими программами и домашним насилием. Коалиция объединяет усилия IT-компаний, НКО, исследовательских институтов и правоохранительных органов в области борьбы с кибersталкингом и помощи жертвам онлайн-насилия.

Сегодня в состав Коалиции входят более 40 организаций, которые делятся друг с другом опытом и вместе работают над решением проблемы цифрового сталкинга. Пользователи, которые подозревают, что за ними следят через мобильное устройство, могут обратиться за помощью на сайте Коалиции, доступном на семи языках.

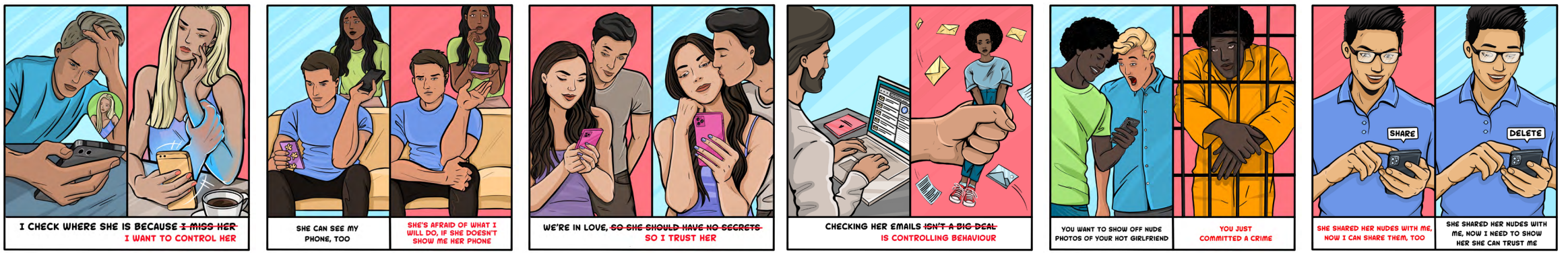
>40

организаций вошли в международную Коалицию по борьбе со сталкерским ПО, сооснователем которой является «Лаборатория Касперского»

«Лаборатория Касперского» сотрудничает также с Европейской сетью по работе с субъектами домашнего насилия[1]. В сентябре 2022 года мы провели глобальную кампанию #NoExcuse4Abuse, направленную на повышение осведомленности общественности о злоупотреблениях технологиями в отношениях. Мы считаем, что очень важно разрушить мифы вокруг этой темы и помочь жертвам распознать признаки возможного цифрового насилия. В рамках кампании были подготовлены комиксы, которые показывают примеры неподобающего поведения в отношениях, замаскированного под проявление «заботы». Главная цель проекта — оспорить аргументацию и оправдания абьюзеров, чтобы удержать их от проявления насилия в отношении своих партнеров.

78,1 тысячи

пользователей были охвачены кампанией #NoExcuse4Abuse



[1] European Network for the Work with Perpetrators of Domestic Violence (WWP EN).

Организуем исследовательские и образовательные проекты против киберсталкинга

Совместно с разными международными компаниями, академическим сообществом и некоммерческими организациями «Лаборатория Касперского» участвует в проведении исследования «Как защитить жертв насилия со стороны партнера от рисков, связанных с цифровыми технологиями»[1]. Для участия в совместном исследовании мы создали партнерство с британским агентством исследований и инноваций UKRI.

Проект стартовал в 2023 году и продлится до 2026 года. «Лаборатория Касперского» поддерживает его своей экспертизой в сфере борьбы с кибернасилием и сталкингом, а также участием в дополнительных мероприятиях.

Уведомляем об угрозе киберсталкинга

Наша Компания первой в отрасли стала предупреждать пользователей своих решений о наличии сталкерского ПО на их устройствах.

В июне 2022 года «Лаборатория Касперского» запустила портал о TinyCheck — бесплатном и безопасном инструменте с открытым исходным кодом для некоммерческих организаций и отделов полиции, которые работают с жертвами цифрового сталкинга. Это решение устанавливается не на смартфон, а на отдельное внешнее устройство — микрокомпьютер Raspberry Pi. TinyCheck может проверить исходящий интернет-трафик, проанализировать его в режиме реального времени и распознать подключения к центрам управления разработчиков сталкерского ПО. При этом решение не позволяет инициатору слежки узнать о такой проверке.

В 2022 году в рамках запуска новой линейки решений для защиты цифровой жизни пользователей мы расширили функции уведомления о нарушении конфиденциальности. Теперь пользователи TinyCheck получают предупреждение не только о наличии сталкерского ПО на устройстве, но и о том, что при его удалении установивший его человек узнает об этом, что может привести к обострению ситуации. Кроме того, жертва сталкинга должна знать, что, удалив приложение, она рискует удалить и важные данные или доказательства, которые могут быть использованы правоохранительными органами.

DeStalk

С 2021 по 2023 год «Лаборатория Касперского» была партнером проекта DeStalk, запущенного в рамках программы EC Rights, Equality and Citizenship («Права, равенство и гражданственность»). Проект объединил пять организаций-партнеров, а также экспертов по кибербезопасности, представителей исследовательских, общественных организаций и органов власти.

На проекте DeStalk мы обучили более 350 профессионалов, которые помогают пострадавшим женщинам и занимаются вопросами насилия, и представителей органов власти. Они изучили действенные методы борьбы с киберсталкингом и научились противостоять другим формам цифрового гендерного насилия. Мы также прикладывали все силы, чтобы сделать доступной для широкой аудитории информацию о цифровом насилии и способах его преодоления.

DeStalk e-learning

В рамках проекта DeStalk «Лаборатория Касперского» разработала электронный учебный курс The DeStalk e-learning по борьбе с кибернасилием и сталкерским ПО на пяти языках. Цель курса — обучить 80–100 профессионалов из 20–30 разных организаций:

- специалистов, работающих с жертвами насилия / пережившими насилие;
- специалистов, работающих с лицами, совершившими насилие в отношении партнера;
- государственных служащих, работающих в сфере борьбы с домашним насилием.

Курс состоял из четырех занятий, которые включали в себя теоретическую часть и тестирование. Первое занятие было посвящено теме цифрового гендерного насилия, второе — формам кибернасилия. На третьем занятии рассматривалась тема сталкинга, на четвертом — работа с жертвами насилия и с его инициаторами. Электронный курс доступен на сайте DeStalk.

DeStalk
detect and stop stalkerware and cyberviolence against women

Более 350 профессионалов
прошли обучение на проекте DeStalk, включая представителей органов власти

130 человек
обучились на курсах по борьбе с кибернасилием и сталкерским ПО

[1] How to protect victims / survivors of Intimate Partner Violence (IPV) from the risks created by digital technologies.

Защищаем от шифровальщиков

Задача

Борьба с программами-вымогателями

По нашим данным, атаки программ-вымогателей становятся все более сложными и причиняют много вреда как компаниям, так и пользователям. Особую опасность вызывают таргетированные (целевые и более сложные) атаки на бизнес — как на крупные компании, так и на малые и средние. Организаторы целевых атак тщательно выбирают мишени — правительства, конкретные организации или отдельные группы людей внутри того или иного предприятия.

Шифровальщики в последние годы остаются одной из наиболее актуальных киберугроз, а их атаки становятся все сложнее. За период с ноября 2022 года по октябрь 2023 года троянцы-шифровальщики атаковали 193 662 уникальных пользователя, в том числе 52 999 пользователей из крупного бизнеса и 6 351 пользователя, связанного с малым и средним бизнесом.

В 2022 году «Лаборатория Касперского» обнаружила две новые кибергруппы вымогателей — RedAlert и Monster. В последнее время их основная цель — повредить как можно больше систем, адаптируя свой вредоносный код одновременно к нескольким ОС. Кроме того, с июля по сентябрь 2022 года Компания обнаружила две волны атак на правительственные организации Албании с использованием программ-вымогателей и вредоносных программ-вайперов. Злоумышленники использовали украденные сертификаты Nvidia и Kuwait Telecommunication для подписи своих вредоносных программ.

Решения «Лаборатории Касперского»

выявили

74,2 млн

атак программ-вымогателей в 2022 году (+20% к 2021 году)

обнаружили

23 364

модификации шифровальщиков и 43 новых семейства программ-вымогателей с ноября 2022 года по октябрь 2023 года[1]

отразили атаки шифровальщиков на компьютерах

193 662

уникальных пользователей с ноября 2022 года по октябрь 2023 года

[1] Источник — https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/11/28132907/KSB_statistics_2023_ru.pdf.

Решения

Разрабатываем продукты для защиты от программ-вымогателей

«Лаборатория Касперского» разработала и опубликовала специальные правила для пользователей, которые хотят защитить себя и свой бизнес от атак программ-вымогателей. Пользователям могут помочь наши продукты, которые продемонстрировали высокую эффективность в защите от программ-вымогателей в результате тестирования[1]. В частности, три решения «Лаборатории Касперского» — Kaspersky Security для бизнеса, Kaspersky Small Office Security и Kaspersky Standard — успешно прошли все тесты, набрав максимальное количество баллов, и получили сертификаты Advanced Approved Endpoint Protection для бизнес-решений и Advanced Certified — для пользовательских.

Предоставляем новейшие данные о киберугрозах

«Лаборатория Касперского» предлагает сервисы информирования о современных киберугрозах, которые помогут любой организации эффективно противостоять им. Сервис Kaspersky Threat Intelligence предоставляет актуальные технические, тактические, операционные и стратегические данные об угрозах, полученные нашими аналитиками и исследователями мирового класса. Благодаря этому «Лаборатория Касперского» стала доверенным партнером правоохранительных и государственных организаций по всему миру, в том числе Интерпола и различных подразделений CERT.

Запросить доступ к этому сервису можно здесь.

158
глобальных пресс-релизов о киберугрозах выпущено Компанией за отчетный период

Помимо этого, Компания постоянно проводит специальные исследования и опросы на разные темы. Это помогает информировать пользователей о киберугрозах, с которыми они могут столкнуться в реальной жизни, даже не подозревая об этом. Так, в отчетном периоде мы рассказали о:

- уязвимостях в популярных «умных» кормушках для домашних животных. Используя обнаруженные уязвимости, злоумышленники могут превратить кормушку в инструмент слежки, а также изменить расписание кормления, тем самым поставив под угрозу здоровье питомца;
- схеме онлайн-мошенничества, ориентированной на владельцев домашних животных, которые хотят купить импортные лекарства для своих питомцев. Через каналы в Telegram мошенники выманивают у них деньги и финансовую информацию;
- ловушках для туристов в период летних отпусков. Тревел-эксперты и специалисты по кибербезопасности предупредили о трех направлениях мошенничества, которые связаны с билетами, размещением туристов и опросами;
- рисках для желающих начать собственный бизнес. «Лаборатория Касперского» выяснила, что 80% россиян недооценивают важность навыков кибербезопасности для старта своего бизнеса, в то время как жертвой кибератаки может стать любая компания, не только крупная;
- новой схеме онлайн-мошенничества, нацеленной на русскоязычных школьников. В коротких видео на YouTube Shorts мошенники рассказывают, как легко зарабатывают много денег, и предлагают поделиться своими идеями со школьниками. Оказалось, что это всего лишь первый этап многоуровневой скам-схемы по выманиванию денег;
- новой кампании по краже криптовалюты через поддельный браузер Tor. Под видом браузера Tor на сторонних интернет-ресурсах злоумышленники распространяют троянца CryptoClipper. При попадании в систему пользователя он регистрируется в автозапуске, маскируясь иконкой какого-либо популярного приложения, например uTorrent. Как только зловред-клиппер обнаруживает в буфере обмена адрес, похожий на криптокошелек, он тут же меняет его на один из адресов, принадлежащих злоумышленнику. С вредоносной кампанией столкнулись более 15 тысяч пользователей в 52 странах, причем больше всего атак было зафиксировано в России;
- технологиях по созданию дипфейк-видео. Наши эксперты обнаружили, что в даркнете предлагают услуги по созданию таких роликов стоимостью до $20 тысяч за минуту. Дипфейки могут создавать для использования в скам-схемах, с целью политических манипуляций, мести и кибербуллинга;
- «Операции Триангуляции» — такое название получила APT-кампания на iOS-устройства с целью шпионажа;
- актуальных спам- и фишинговых атаках: статистика и тенденции, которым следовали злоумышленники в 2023 году, в новом отчете.

Кроме того, мы создали обучающие видео, где рассказываем о криптофишинге, провели вебинар о существующих угрозах в этой области, а также выпустили собственное исследование на эту тему.

[1] Тестирование AV-TEST проходило в августе 2023 года.

Как мы раскрыли «Операцию Триангуляцию»

Вместе против шпионажа

В начале июня 2023 года исследователи «Лаборатории Касперского» обнаружили ранее неизвестное вредоносное ПО, которое атакует устройства с операционной системой iOS. Это целевые атаки в рамках APT-кампании, которая получила название «Операция Триангуляция» (Operation Triangulation). Зловред проникает на устройства жертв с помощью эксплойта, доставляемого в скрытом сообщении iMessage, после этого он самостоятельно запускается и получает полный контроль над устройством и пользовательскими данными. Цель злоумышленников — шпионаж.

Специалисты установили, что внедренное шпионское ПО незаметно передает информацию с устройства жертвы на удаленные серверы. Злоумышленников интересовали записи с микрофонов, фотографии из мессенджеров, геолокация и данные о других действиях владельца.

«Сегодня у нас очень большая и важная новость. Экспертами нашей Компании была обнаружена крайне сложная, профессиональная целевая кибератака с использованием мобильных устройств производства Apple», — написал в своем блоге Евгений Касперский.

По его словам, косвенным признаком присутствия Triangulation на устройстве является блокировка возможности обновления iOS. Для более точного распознавания заражения потребуется снять резервную копию устройства и проверить ее специальной бесплатной утилитой.

Узнать больше об «Операции Триангуляция» и том, как проверить, заражено ли iOS-устройство, можно на портале Securelist.

Что в результате?

«Лаборатория Касперского» разработала утилиту triangle_check для компьютеров на операционных системах Windows и Linux, с помощью которой пользователи могут проверить свой iPhone (бэкап системы) на факт заражения вредоносным ПО Operation Triangulation. Для проверки с помощью этой утилиты на Windows и Linux достаточно скачать бинарную сборку, а на macOS е можно установить ее как Python-пакет.

Специалисты компании Apple, в свою очередь, признали проблему и выпустили обновления, которые устраняют допущенные уязвимости.

GRI 203-1

NO MORE RANSOM

Чтобы противодействовать злоумышленникам, по инициативе «Лаборатории Касперского» в 2016 году был создан альянс No More Ransom, куда помимо нашей Компании вошли Европол, нидерландская полиция и вендоры из кибербезопасности. Участники альянса обмениваются опытом, знаниями и decryption tools — инструментами дешифровки, которые помогают восстанавливать данные, зашифрованные вымогателями.

Наш вклад в инициативу No More Ransom

Вместе против программ-вымогателей

360 000
раз были скачаны бесплатные инструменты для дешифровки

с их помощью можно расшифровать файлы, заблокированные
39
семействами программ-вымогателей

более **2 млн**
пользователей смогли восстановить данные

Международная инициатива No More Ransom, одним из основателей которой является «Лаборатория Касперского», создана с целью помочь жертвам троянцев-вымогателей снова получить доступ к своим зашифрованным данным, не выплачивая денег атакующим.

Этот проект представляет собой уникальное партнерство между правительственными организациями, правоохранительными структурами, антивирусными компаниями и образовательными учреждениями.

Участники инициативы разрабатывают бесплатные инструменты для дешифровки, рассказывают о рисках, связанных с атаками программ-вымогателей, а также о лучших практиках для противодействия им. В марте 2023 года «Лаборатория Касперского» выпустила новую версию инструмента для дешифровки в помощь жертвам модификации программы-вымогателя, основанной на утекшем ранее коде программы Conti.

Недавно No More Ransom отметила важную веху: более 2 млн пользователей получили возможность восстановить данные благодаря инициативе.

Что в результате?

Совместными усилиями нам удалось сделать цифровую среду более безопасной: мы помогли сотням тысяч пользователей и снизили общий уровень угроз в онлайн-мире.

Бесплатные инструменты «Лаборатории Касперского» для дешифровки, доступные в рамках инициативы No More Ransom, были скачаны более 360 тысяч раз за пять лет. С их помощью можно расшифровать файлы, заблокированные 39 семействами программ-вымогателей. Эти инструменты предоставили жертвам средства для восстановления важных данных без необходимости выполнять требования преступников. Такой результат говорит об успехе инициативы.

Обучаем пользователей основам кибербезопасности

Задача

Предоставление пользователям инструментов самозащиты

Умение обеспечить свою безопасность в цифровом пространстве становится важным навыком современного человека. Обучая наших пользователей основам кибербезопасности, мы не только помогаем им распознавать потенциальные угрозы, но и предоставляем инструменты для собственной защиты. Таким образом мы инвестируем в безопасное цифровое будущее для всех.

Решения

Kaspersky Academy

>8 000

студентов обучились в Kaspersky Academy за 2022–2023 годы

Еще в 2010 году мы запустили Kaspersky Academy, чтобы масштабировать образовательные инициативы и сделать их доступными для всех желающих. Мы планировали превратить ее в глобальный университет, где будут собраны все обучающие материалы, касающиеся информационной безопасности. И нам удалось реализовать этот проект.

Сейчас спикерами Kaspersky Academy выступают руководители команд Компании, директора направлений, ведущие специалисты и приглашенные эксперты в области информационной безопасности. За 2022–2023 годы в Kaspersky Academy прошли обучение более 8 000 студентов из России, Европы, Саудовской Аравии, Руанды и других стран.

Преимущества Kaspersky Academy:

- один из механизмов получения доступа к контенту — платформа Education.kaspersky.com;
- адаптирована под два формата продуктов:
  1. видеоуроки + тестовые задания + сертификат;
  2. видеоуроки + прямые эфиры + тестовые задания + финальный тест + сертификат;
  3. формат онлайн рабочей тетради с автопроверкой + сертификат;
- позволяет отслеживать результаты студентов — промежуточные и финальные;
- оповещает студентов о предстоящем вебинаре;
- позволяет быстро кастомизировать формат тренинга и сбор аналитики под запрос заказчика и проект;
- дает возможность управлять длительностью доступа учащегося к платформе.

В 2023 году были запущены курсы:

- «Введение в кибербезопасность». Обновленный флагманский курс для русскоязычной аудитории, который рассматривает все основные аспекты информационной безопасности. Он ориентирован как на IT-специалистов или студентов, так и на частных пользователей;
- «Кибербезопасность для топ-менеджеров». Курс дает слушателям представление о кибербезопасности как системе и показывает, как киберриски влияют на бизнес и как можно ими управлять.

Ключевые проекты Academic Affairs для школьников и студентов в 2023 году:

SafeBoard — 15+ направлений IT-стажировки (более 500 студентов присоединились к программе с 2016 года). За восемь лет существования этой программы более половины ее участников перешли в штат Компании и сейчас работают в том числе на ступенях Middle, Senior и Lead;

Secure'IT Cup — ежегодный международный конкурс студенческих проектов в сфере кибербезопасности (30+ стран-участниц, более 2 000 заявок от студентов каждый год);

Долина технологий — летняя практика для школьников и студентов колледжей (более 1 200 регистраций в 2023 году, 45 участников прошли практику в офисе);

Cyber Generation — тренинг-программа для студентов и недавних выпускников Саудовской Аравии (91 участник);

Kaspersky Academy Alliance — специальная программа для университетов, позволяющая интегрировать экспертизу в области кибербезопасности и новейшие технологии Kaspersky в процесс обучения студентов.

«Лаборатория Касперского» делится практическими знаниями со студентами

почти 200 университетов

по всему миру в 42 странах.

Более 60 учебных заведений из этого числа находятся в России и СНГ.

Тренинги по кибербезопасности для НКО

GRI 203-1

Кибербезопасность важна для эффективной деятельности некоммерческих организаций (НКО), которые значительно зависят от цифровых технологий. «Лаборатория Касперского» регулярно проводит тренинги для некоммерческих организаций, чтобы повысить уровень их защиты от онлайн-угроз, которые постоянно эволюционируют. Такое партнерство способствует созданию более безопасного и устойчивого цифрового будущего для всех.

В 2022–2023 годах мы организовали тренинги на разные темы для российских и международных некоммерческих организаций:

- **Киберсталкинг**. Наши ведущие исследователи угроз информационной безопасности провели два тренинга по проблеме кибersталкинга для фонда «Благие дела» из Казани и Нижегородского женского кризисного центра, который оказывает бесплатную психологическую и юридическую поддержку людям, столкнувшимся с насилием и жестоким обращением. Также для этих организаций мы провели тренинг по использованию бесплатного open-source-инструмента TinyCheck, который способен обнаружить установленное на девайс ПО для слежки, не уведомляя об этом сталкера. Теперь в Нижегородском женском кризисном центре каждая женщина может проверить свое устройство на предмет обнаружения такого ПО.

- **Доксинг**[1]. Вместе с Сингапурским советом женских организаций[2] мы провели бесплатный семинар по борьбе с доксингом. Наши специалисты рассказали, как можно снизить риски неправомерного использования личной информации, защитить свои и чужие личные данные, познакомили слушателей с надежным защитным программным обеспечением и раскрыли возможные мотивы злоумышленников.

- **Кибергигиена**. В партнерстве с платформой социальных изменений todogood мы провели онлайн-интенсив на тему кибергигиены в рамках программы «Я могу» для уязвимых групп населения — женщин, попавших в сложную жизненную ситуацию, людей с ограниченными возможностями здоровья и людей старшего возраста. Цель программы — помочь участникам в профессиональной переподготовке, адаптации к обучению, работе в онлайн-среде, социально-культурным изменениям и новым технологиям. В записи и онлайн интенсив прошли 946 человек, которые сдали тест и получили сертификаты.

Мы также создали ряд проектов по кибербезопасности в партнерстве с международными организациями. В частности, был запущен Kids' Cyber Resilience Project, который активно развивался в странах Азиатско-Тихоокеанского региона с марта 2023 года. В рамках этого проекта мы провели ряд важных мероприятий, нацеленных на повышение грамотности местного населения в сфере кибербезопасности.

- Совместно с Centre For Cybersecurity и The HEAD Foundation «Лаборатория Касперского» запустила в Сингапуре свой глобальный проект «**Киберустойчивость для детей**» с панельной дискуссией о том, как совместный и проактивный подход к онлайн-безопасности может принести пользу детям в цифровой среде. В проекте участвуют родители, преподаватели, учащиеся, НКО и представители правительства.

- **Онлайн-семинары по киберустойчивости** для преподавателей в Азиатско-Тихоокеанском регионе (APAC) в партнерстве с Coalition Against Bullying for Children & Youth (CABCY). В рамках серии вебинаров мы более подробно рассмотрели тему буллинга и кибербуллинга. CABCY помогла участникам разобраться в этой сложной проблеме и понять роль взрослых в поддержке детей.

- **Face-to-Face** — семинар по киберустойчивости для преподавателей в Маниле, проведенный в сентябре 2023 года совместно с отделом школьного образования в Валенсуэле Департамента образования Филиппин в рамках глобального проекта «Лаборатории Касперского» Kids' Cyber Resilience. Цель семинара — помочь филиппинским преподавателям изучить основы кибергигиены, ознакомиться с бесплатными инструментами и ресурсами «Лаборатории Касперского» для обучения детей онлайн-безопасности в классе.

- **Cyber Resilience Day**. В сотрудничестве с городским советом Петалинг-Джая в Малайзии «Лаборатория Касперского» провела интерактивный тренинг по осведомленности о кибербезопасности и киберустойчивости для более чем 250 учащихся и учителей, представляющих десять государственных школ.

- **Семинар по кибербезопасности в Индии**. В партнерстве с Фондом ISAC «Лаборатория Касперского» провела семинар по кибербезопасности для 150 учителей, представляющих более 30 школ. Семинар был организован школой Air Force Bal Bharati в Дели.

[1] Doxing — практика публичного раскрытия личной информации о человеке в интернете без его согласия.
[2] The Singapore Council of Women's Organisations (SCWO).

Наш вклад в формирование здорового цифрового поведения

Учим защищаться от цифровых угроз, слушая подкаст

Подкаст «Смени пароль!» — документально-разговорное шоу про информационную безопасность, которое ведут журналист и писатель Алексей Андреев, главный эксперт «Лаборатории Касперского» Сергей Голованов и главный технологический эксперт «Лаборатории Касперского» Александр Гостев.

Подкаст выходит с 2021 года и насчитывает три сезона. Его можно найти на всех популярных подкаст-платформах, включая Apple Podcasts, «Яндекс Музыка», Google Podcasts, VK, Castbox, YouTube.

Ведущие подкаста «Смени пароль!» обсуждают насущные вопросы из мира цифровой безопасности и помогают слушателям разобраться в актуальных киберугрозах для пользователей и бизнеса.

- Куда утекают персональные данные?
- Чем опасен интернет вещей?
- Искусственный интеллект — защита или угроза?

Ответы на эти и многие другие вопросы дают ведущие проекта и приглашенные эксперты. В гостях у подкаста уже побывали представители Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) и крупнейших компаний, таких как «Ростелеком», «Яндекс», «Билайн», OZON, «Газпром-медиа», Райффайзен Банк и Хоум Банк.

Помимо дискуссий в формате аудио, в проекте есть практика очных встреч со слушателями. Так, осенью 2023 года открытая запись подкаста «Смени пароль!» стала первым мероприятием Дискуссионного клуба Музея криптографии. Эксперты обсудили, чем русские шифры отличаются от зарубежных, какая криптографическая защита нужна современному человеку и почему квантовые компьютеры напоминают «яблони на Марсе», а также ответили на многочисленные вопросы слушателей.

Что в результате?

>400 000 раз

прослушан подкаст за три сезона

За три года подкаст стал источником актуальной информации об угрозах цифрового мира. Сегодня «Смени пароль!» помогает слушателям создавать более безопасное онлайн-пространство вокруг себя и своего бизнеса.

- Количество прослушиваний третьего сезона в конце 2023 года превысило 100 000, всего подкаст послушали более 400 000 раз.
- С 2022 года «Смени пароль!» регулярно попадает в топ подкастов про технологии на Apple Podcasts и «Яндекс Музыке», а также в тематические подборки от ведущих медиа.
- В 2023 году проект стал финалистом PROBA Awards и Премии Рунета.

Обеспечиваем онлайн-безопасность детей

Задача

Защита детей в цифровом мире

«Лаборатория Касперского» несколько лет подряд регулярно проводит опрос по детской онлайн-безопасности. Компания делает это, чтобы понять, как интернет влияет на юных пользователей, чем они интересуются и с какими неприятностями могут столкнуться в Сети.

Согласно опросу 2022 года, проведенному по заказу «Лаборатории Касперского» в крупных городах России[1], 77% детей возраста от 7 до 10 лет познакомились с гаджетами еще до школы. По данным нового опроса, который Компания провела в 2023 году, у подавляющего числа школьников начальных классов (88%) сейчас есть собственный телефон или планшет. Практически каждый старшеклассник имеет собственный гаджет. Начиная со средней школы заметная часть детей проводит в гаджетах практически все свободное время. Родители беспокоятся о том, с кем общается в интернете их ребенок, не сталкивается ли он с агрессией в свой адрес, какие сайты посещает.

88%

младших школьников имеют свой телефон или планшет

55%

детей за последний год сталкивались в интернете с жестокими видео или роликами со взрослым содержанием

29%

родителей не знают, какая информация об их детях есть в открытом доступе в интернете

«Чтобы оградить детей от самых разных онлайн-угроз, необходимо сочетать технические и нетехнические меры защиты. К первым относятся специальные настройки, например семейные аккаунты, программы родительского контроля, антивирус и автоматические определители номеров. К нетехническим — постоянное повышение цифровой грамотности, в том числе в вопросах информационной безопасности. Обучать детей основам цифровой гигиены важно с самого раннего возраста. Со временем это станет эффективнее, чем одни только родительские запреты».

Андрей Сиденко,
руководитель направления «Лаборатории Касперского» по детской онлайн-безопасности

[1] Участниками опроса стали более 1 000 пар родитель — ребенок.

Решения

Обучаем детей основам кибербезопасности

Создание безопасной онлайн-среды для детей — задача первостепенной важности, от которой зависит наше будущее. «Лаборатория Касперского» работает над этой задачей как своими силами, так и в партнерстве с министерствами, ведомствами и другими организациями по всему миру.

Чтобы понять, как интернет влияет на юных пользователей, чем они интересуются и с какими неприятностями могут столкнуться в Сети, «Лаборатория Касперского» несколько лет подряд проводит опросы и исследования по детской онлайн-безопасности. Вот некоторые из них, представленные в отчетном периоде.

- **«Взрослые и дети в интернете»** — серия опросов по детской онлайн-безопасности и одноименный отчет. В 2022 году опрос проводила компания Online Interviewer по заказу «Лаборатории Касперского» в мае — июне 2022 года. Всего было организовано 2 008 онлайн-интервью, в которых приняли участие 1 004 пары родитель — ребенок в возрасте от 3 до 18 лет, в крупных городах России. Темы для интервью были выбраны так, чтобы отразить ситуацию в самых разных сферах онлайн-жизни. Полученные результаты вместе с комментариями эксперта «Лаборатории Касперского» по детской онлайн-безопасности помогли взрослым лучше понять интересы юных пользователей и показали, как можно сделать цифровой мир более безопасным для них.

- **Новый опрос по детской онлайн-безопасности**. В мае — июне 2023 года специалисты Online Interviewer провели для нас новое исследование, чтобы выяснить, как обстоят дела с детской онлайн-безопасностью. Они организовали 2 032 онлайн-интервью (всего было опрошено 1 016 пар родитель — ребенок). В результате была получена такая статистика:

  - 29% родителей не знают, какая информация об их детях есть в открытом доступе в интернете;
  - больше половины (55%) детей, по их словам, за последний год сталкивались в интернете с жестокими видео или роликами со взрослым содержанием;
  - треть родителей хотят, чтобы их ребенок работал в сфере IT, когда вырастет. При этом среди детей доля тех, кто хотел бы в будущем работать в этой отрасли, еще выше — 41%;
  - 30% опрошенных родителей в России волнует проблема детской интернет-зависимости. Больше половины (54%) считают, что современные дети зависимы от гаджетов и интернета;
  - начиная с семи лет большинство детей проводят в интернете более часа в день;
  - больше половины родителей (53%) уверены, что через 10–15 лет сенсорные экраны и доски в школах заменят привычные инструменты проведения урока, 39% отметили, что вместо учебников будут планшеты, а 37% считают, что в будущем в обучении будут использоваться голосовые помощники.

- **Дети в интернете — 2022**. «Лаборатория Касперского» регулярно проводит глобальные исследования по теме детской онлайн-безопасности. В основу исследований ложится анонимизированная статистика, собранная решением Kaspersky Safe Kids.

Также в отчетном периоде мы организовали ряд образовательных мероприятий и проектов по кибербезопасности для школьников, учителей и родителей.

- **«Мама, я буду блогером!»**. В июне 2022 года «Лаборатория Касперского» запустила собственный интерактивный мини-сериал «Мама, я буду блогером!». Он состоит из десяти серий по 2–3 минуты, которые выходили до конца 2022 года. Благодаря сериалу вместе с главной героиней Милой дети узнали, как безопасно записывать вайны, избегать мошенников и хейтеров, как отличить фишинговый сайт от настоящего и почему важно следовать правилам этикета в Сети.

- **«Урок цифры»**. В 2022 и 2023 годах «Лаборатория Касперского» продолжила участие в акции «Урок цифры», которую проводит АНО «Цифровая экономика» при поддержке Министерства просвещения Российской Федерации (Минпросвещения России) и Минцифры России. На уроках Компании в 2022 году дети знакомились с темой «Исследование кибератак», а в 2023 году они обучались мобильной безопасности. За 2023 год школьники прошли урок более 2 млн раз. Они узнали, каким бывает вредоносное ПО для мобильных устройств, как обезопасить свои данные в интернете, а также познакомились с миром профессий в области кибербезопасности.

Подробнее о проекте читайте на с. 105

- **«Цифровой ликбез»**. «Лаборатория Касперского» и АНО «Цифровая экономика» при поддержке Минпросвещения России и Минцифры России создали серию коротких мультфильмов для детей про цифровую безопасность и приватность. В 2023 году они пополнили подборку полезных материалов всероссийского просветительского проекта «Цифровой ликбез».

- **Курс для школьников по кибербезопасности**. В октябре 2023 года «Лаборатория Касперского» открыла всем желающим доступ к первым материалам курса «Основы информационной безопасности» для учеников седьмого класса. Через некоторое время будет доступен курс для школьников 8–11-х классов. Это практико-ориентированный курс, его могут использовать учителя на уроках информатики и в рамках внеурочной деятельности, а также родители и сами учащиеся.

- **Образовательные мероприятия для учеников и учителей в России и странах СНГ**. В 2022–2023 годах было проведено более 150 онлайн- и офлайн-мероприятий для учащихся и учителей средних общеобразовательных школ, а также для родителей в 26 регионах России и в странах СНГ.

- **Kaspersky Safe Family Spain**. 35 спектаклей по книге «Kasper, Sky и зеленый медведь», обучающей основам кибербезопасности, были поставлены для 3 684 учеников испанских школ в рамках инициативы Safe Family.

- **#ShareAware Hub**. «Лаборатория Касперского» помогает родителям и детям повысить их безопасность в интернете с помощью советов и подсказок. На хабе представлено множество полезных материалов об использовании мультимедиа в интернете.

- **Kids on the Internet** — разработанный Компанией курс о безопасности детей в интернете. Он предназначен для детей и их родителей, а также для всех, кто использует интернет.

- **Hacker:HUNTER**. Компания приняла участие в производстве сериала о реальных киберинцидентах. В 2023 году вышел новый сезон, который посвящен тому, как злоумышленники вовлекают детей в свою деятельность и растят из них хакеров и как правоохранительные органы противостоят им.

- **«Киберазбука»**. Чтобы помочь детям и их родителям развивать цифровую грамотность, эксперты Компании подготовили познавательную книгу для детей и их родителей о популярных явлениях из мира технологий с советами о том, как защититься от распространенных цифровых угроз. В книге от А до Я читатели знакомятся с новыми технологиями, распространенными киберрисками и инструментами для защиты от них. «Киберазбука» доступна на английском языке для скачивания всеми желающими на сайте Компании. Позднее будут доступны также версии азбуки на русском, французском, итальянском и испанском языках.

В 2023 году проект «Взрослые и дети» — весь комплекс мероприятий «Лаборатории Касперского» по онлайн-безопасности детей и их родителей — стал финалистом премии Proba Awards.

Сотрудничаем с IT-компаниями и регуляторами для защиты детей в интернете

Мы стремимся сделать онлайн-пространство, в котором живут современные дети, как можно более безопасным. «Лаборатория Касперского» — один из основателей Альянса по защите детей в цифровой среде, который был создан крупнейшими IT-компаниями России в сентябре 2021 года.

В 2022 году в рамках Альянса «Лаборатория Касперского», «Яндекс» и VK запустили пилотный проект по выявлению и блокировке контента, связанного с распространением детской порнографии, а также так называемого сексуализированного контента с участием несовершеннолетних.

В октябре 2023 года Альянс по защите детей в цифровой среде провел в Казани роуд-шоу «Маршрут построен: тропы безопасности в Сети», на котором были озвучены результаты исследования «Лаборатории Касперского»: большинство родителей в России (87%) предпринимают те или иные меры, чтобы оградить своего ребенка от опасностей в интернете. Однако выяснилось, что только 48% взрослых сами следуют всем установленным правилам, что снижает эффективность этих мер. Эксперты Компании напомнили родителям о необходимости быть хорошим примером для детей и составили чек-лист с рекомендациями, на что обратить внимание при выборе подходящего решения родительского контроля.

В декабре 2023 года Альянс по защите детей в цифровой среде организовал в Санкт-Петербурге двухдневный образовательный марафон «Безопасная цифра», посвященный правилам безопасного поведения в интернете. Гости марафона — в основном дети и подростки — могли поучаствовать в IT-квизе, тематических мастер-классах, круглых столах и семинарах. Родители и учителя обсудили вопросы цифровой безопасности. Также была организована деловая программа с участием IT-экспертов, представителей органов власти, бизнеса и общественных организаций. В марафоне участвовали основатели Альянса — «Лаборатория Касперского», «Яндекс», VK, «Ростелеком», «Билайн» и «МегаФон».

Kaspersky Safe Kids

Мы стремимся защитить детей от онлайн-угроз и создать условия, в которых ребенок сможет максимально безопасно пользоваться интернетом. Для этого мы предлагаем наше решение Kaspersky Safe Kids — приложение родительского контроля, которое ограждает ребенка от контента, не соответствующего его возрасту, и помогает формировать полезные цифровые привычки. Решение представлено в том числе в бесплатной версии.

Основные функции Kaspersky Safe Kids

Безопасный поиск
Приложение взаимодействует с поисковыми системами и блокирует нежелательные запросы. Раз в неделю родители получают отчеты о том, что искал ребенок в интернете.

Контроль использования приложений
Базовая функция — блокировка приложений, которые не подходят ребенку. Также предусмотрен контроль времени использования (можно настроить временные интервалы и назначить выходные дни).

Контроль экранного времени
Приложение позволяет установить разрешенное количество часов экранного времени в день и заблокировать устройство, если лимит достигнут. Также можно отключать устройство в определенные промежутки времени.

Установка безопасного периметра
Благодаря опции с GPS приложение отправляет уведомление родителям, если во время учебы ребенок покинул установленную локацию (например, школу).

Мониторинг потенциально опасных контактов в соцсетях
Родители не могут читать сообщения ребенка, но приложение уведомляет их о самом факте переписки и дает возможность увидеть профиль собеседника.

В 2023 году мы дважды обновили решение Kaspersky Safe Kids. В новых версиях усовершенствованы дизайн и интерфейс приложения, появился новый функционал управления экранным временем, добавились видео с советами по воспитанию детей, легкой настройке функций и другой полезной для родителей информацией. Приложение можно установить на стационарные компьютеры и мобильные устройства со всеми популярными операционными системами. Дети теперь могут запрашивать у родителей дополнительное время на использование устройства, а родителям достаточно одобрить или отклонить запрос.

7
наград AV-TEST

7
наград AV-Comparatives

>1 млн
скачиваний по всему миру

106 млн
заблокированных сайтов

Результаты тестирования Kaspersky Safe Kids

По данным отчета независимой лаборатории AV-TEST, вышедшего в январе 2023 года, Kaspersky Safe Kids заблокировал:

- 92% потенциально неприемлемых ресурсов на Windows (по сравнению с 90% в 2021 году);
- 87% потенциально неприемлемых ресурсов на Android (в 2021 году — 85%);
- почти 100% нежелательного контента «для взрослых» на Windows.

Наш вклад в защиту детей в киберпространстве

Обучаем кибербезопасности со спектаклем «Kasper, Sky и зеленый медведь»

Число детей, использующих цифровые технологии, постоянно увеличивается. Вместе с этим в киберпространстве распространяются новые формы цифровых угроз, особенно опасные для детей из-за отсутствия у них опыта и знаний о таящихся там угрозах. Киберзапугивание, секс-вымогательство и другие виды притеснений стали проблемой, от которой дети и подростки страдают каждый день, поэтому «Лаборатория Касперского» сделала своей целью обеспечение их защиты в онлайн-мире.

В рамках инициативы Safe Family Компания запустила в Испании спектакль «Kasper, Sky и зеленый медведь» — адаптацию книги Марлис Слегерс для детей в возрасте от 6 до 9 лет, которая знакомит их с цифровым миром и учит использовать интернет безопасно. «Лаборатория Касперского» превратила эту книгу в кукольное представление, которое не только обучает детей, но и стремится донести до учителей и родителей, что киберугрозы сегодня выходят за рамки простого вируса.

Благодаря усилиям «Лаборатории Касперского» тысячи детей, педагогов и родителей обучились безопасному использованию интернета. А кампания «Kasper, Sky и зеленый медведь» была удостоена наград на церемонии Social Business Awards 2019:

- «Лучший ответственный проект в сфере защиты детей»;
- «Лучший проект социальной ответственности в сфере кибербезопасности»;
- «Лучший ответственный проект в борьбе с буллингом».

Кроме того, фонд Gala Acción Social наградил «Лабораторию Касперского» знаком отличия «Компания с лучшими действиями в борьбе за защиту детей».

Что в результате?

16 805 детей

в **106** школах

просмотрели спектакль с момента запуска проекта в 2018 году

В течение 2022/2023 учебного года в рамках инициативы состоялось

35 представлений, которые посетили

3 684 ученика.

[1] Ближний Восток, Турция и Африка.

Наши достижения

«Лаборатория Касперского» в Испании получила награды Social Business Awards 2023 за свою деятельность в области борьбы с цифровым гендерным насилием. Компания была удостоена наград в следующих категориях: «Лучшая корпоративная социальная ответственность в секторе кибербезопасности», «Лучшая инициатива по предотвращению гендерного насилия в секторе кибербезопасности» и «Лучший проект по интернет-безопасности в секторе кибербезопасности». Кроме того, организатор премии Gala Acción Social присудил Компании специальную награду за лучшие инициативы в области кибербезопасности, а также назвал ее Платиновой компанией и Компанией года.

Наши планы на 2024 год

- Развитие партнерства с международными правоохранительными организациями, коалициями и НКО, нацеленного на борьбу со сталкингом.
- Выпуск нового отчета о состоянии сталкерского ПО.
- Запуск курса по кибергигиене на двух языках.
- Начало продвижения проекта Kids Cyber Resilience в регионах СНГ и МЕТА[1].
- Выпуск аналитического отчета по детской онлайн-безопасности с данными опроса за 2023 год.
- Публикация «Киберазбуки» для самых юных пользователей на русском, испанском, итальянском и французском языках.