

Как мы защищаем разные группы пользователей

GRI 3-3

Защита разных групп пользователей — важная часть нашей работы по созданию более безопасного цифрового пространства.

Боремся с киберсталкингом

Что такое стalkerское ПО и чем оно опасно

Современные технологии стали важной частью жизни и во многом помогают нам, но иногда их используют во вред. Одна из таких угроз — цифровое преследование или киберсталкинг.

Злоумышленники могут установить на смартфон жертвы специальное приложение — так называемое стalkerское ПО (stalkerware). Такое ПО работает скрытно и тайно следит за человеком через его устройство: собирает информацию о местоположении, читает переписки, получает доступ к фотографиям и другим личным данным без ведома владельца смартфона. Это серьезная проблема, причем не только техническая, но и социальная, поскольку она нарушает право человека на приватность и часто может быть связана с домашним насилием.

Масштаб проблемы

23%

посетителей мировых сервисов онлайн-знакомств сталкивались с онлайн-преследованием

34 тысячи

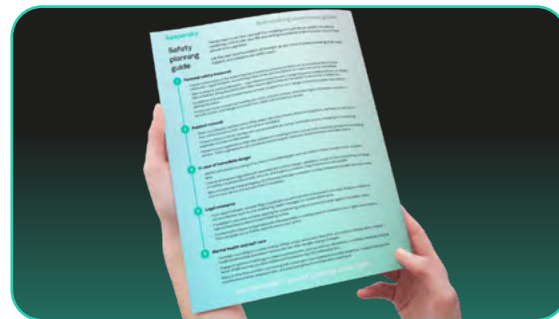
пользователей во всем мире [столкнулись](#) со стalkerским ПО в 2024–2025 годах

¹ В исследовании участвовали 21 000 человек по всему миру.

Исследования «Лаборатории Касперского» показывают, что цифровое преследование — актуальная угроза.

[Опрос](#), проведенный Компанией в России, выявил отношение респондентов к различным формам цифрового преследования со стороны бывших или нынешних партнеров, — вне зависимости от того, сталкивались респонденты с подобным или нет. Больше половины опрошенных боятся ситуаций с требованием предоставить доступ к личным данным на смартфоне, примерно столько же — слежки через стalkerские программы и трекеры (беспроводные метки). При этом последние два способа слежки сильнее беспокоят женщин, чем мужчин. Проблема цифровой слежки не ограничивается одной страной: по результатам [глобального исследования](#) «Лаборатории Касперского»¹, примерно каждый четвертый пользователь сервисов онлайн-знакомств (23%) сталкивался с той или иной формой цифрового преследования.

Обнаружить стalkerские приложения без специальных средств очень трудно. В случае обнаружения подозрительного приложения эксперты советуют не удалять его сразу (преследователь может быстро узнать об этом), а обратиться за помощью к специалистам, в кризисный центр или полицию.



Помогаем пользователям защищать себя

«Лаборатория Касперского» уже много лет защищает пользователей от цифрового преследования, возглавляя борьбу с киберсталкингом. В 2019 году мы внедрили в наше мобильное приложение функцию обнаружения стalkerских программ. Наше решение [Kaspersky для Android](#) сканирует устройство и предупреждает пользователя при выявлении скрытых приложений для слежки.

В 2024 году мы пошли дальше и добавили в приложение функцию [«Кто за мной следит?»](#), которая усиливает защиту сразу на нескольких уровнях. Она находит в телефоне незаметно установленные стalkerские приложения, обнаруживает поблизости подозрительные Bluetooth-метки и другие устройства слежения, а также показывает, какие разрешения выданы приложениям, нет ли среди них лишних, упрощающих слежку. Благодаря этому пользователь может вовремя заметить угрозу и сохранить контроль над своей безопасностью.

Помимо технических решений против сталкинга, Компания уделяет большое внимание просвещению и сотрудничеству.

В ноябре 2024 года мы опубликовали «Руководство по противодействию преследованию» — [Anti-Stalking Awareness Guide](#), созданное совместно с международными экспертами и жертвами сталкинга. Цель инициативы — поддержать пострадавших и их близких, повысить осведомленность о проблеме и предоставить практические инструменты для защиты. Руководство помогает разобраться в природе сталкинга, опровергает распространенные мифы и описывает манипулятивные методы, которые используют преследователи. Центральное место в нем занимают два практических чек-листа, охватывающие как цифровую, так и физическую безопасность.

Первый чек-лист включает рекомендации по составлению плана безопасности, форму для документирования инцидентов, а также советы для родственников и друзей, поддерживающих пострадавших. Он был создан при участии:

- Олимпии Корал Мело Крус — активистки, инициировавшей «Закон Олимпии» в Латинской Америке, который стал основой для борьбы с цифровым насилием;
- Марсели Эрнандес — соосновательницы Red Latinoamericana de Defensoras Digitales, сети поддержки защитников цифровых прав;
- Жанаины Кампос — бразильского психоаналитика, работающего с дисфункциональными отношениями;
- Акасии Дианы и Юлии Павловой — жертв stalking, которые поделились личными историями, чтобы повысить осведомленность других женщин.

Второй чек-лист — гид по цифровой безопасности ([Digital Security Guide](#)), разработанный экспертом «Лаборатории Касперского» Анной Ларкиной, — содержит рекомендации по защите личных данных, настройке приватности и снижению цифровых рисков, которые могут сделать человека уязвимым к онлайн-преследованию. Вместе эти материалы формируют целостный подход к поддержке пострадавших, охватывая как защиту физической безопасности, так и обеспечение цифровой защиты, и подчеркивают приверженность «Лаборатории Касперского» созданию более безопасного цифрового пространства для всех.

Кроме того, эксперты Компании регулярно делятся советами по цифровой безопасности. Например, мы рекомендуем использовать сложные уникальные пароли и не делиться ими, тщательно настраивать приватность в соцсетях и не раскрывать слишком много личной информации в интернете. Такие простые меры снижают риски и помогают чувствовать себя увереннее.

Объединяем усилия и помогаем жертвам

>40

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

Противодействие киберсталкингу требует объединения усилий многих участников, и Компания активно работает в этом направлении. В 2019 году мы стали сооснователем международной Коалиции по борьбе со сталкерским ПО ([Coalition Against Stalkerware](#)), которая сегодня объединяет более 40 организаций — от IT-компаний до правоохранительных органов. Вместе с партнерами мы повышаем осведомленность о цифровом насилии и помогаем пострадавшим.

«Лаборатория Касперского» участвует в международных инициативах по борьбе с цифровым насилием, например в европейском проекте DeStalk. Еще один совместный проект — исследование «Как защитить жертв насилия со стороны партнера от рисков, связанных с цифровыми технологиями»¹. Кроме «Лаборатории Касперского», в нем участвуют другие международные компании, представители академического сообщества и некоммерческие организации. Проект реализуется в партнерстве с британским агентством [UKRI](#) с 2023 по 2026 год. Компания поддерживает его своей экспертизой в области противодействия кибернасилию и stalking, а также участием в дополнительных мероприятиях.

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

Безопасное пространство для тех, кому нужна защита

Поддерживаем [Нижегородский женский кризисный центр](#)

Мы понимаем, что за каждой цифрой статистики стоят реальные судьбы, поэтому стараемся участвовать в инициативах по помощи жертвам в реальной жизни.

Проблема

Женщины и дети, столкнувшиеся с домашним насилием и преследованием, часто нуждаются в срочном и безопасном убежище. При этом иногда у пострадавших нет доступа даже к собственным документам и деньгам. В такой ситуации во многих регионах у них нет шансов найти экстренное убежище.

Что сделано

С 2022 года «Лаборатория Касперского» поддерживает проект «Безопасная квартира» Нижегородского женского кризисного центра. Это секретное жилье, куда пострадавшие могут заселиться прямо в день обращения. Подопечным предоставляются базовые вещи: проживание, питание, одежда, связь, а также психологическая, юридическая и социальная помощь. Проект работает без формальных барьеров даже при отсутствии документов.

Результат

За четыре года фонду удалось помочь 32 женщинам с детьми.



Обеспечиваем онлайн-безопасность детей

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

Почему это важно

Дети сегодня начинают пользоваться интернетом с самого раннего возраста — для учебы, общения и развлечений. Онлайн-среда дает много возможностей для развития, но вместе с тем несет и реальные риски: угрозы мошенничества, кибербуллинга, опасного контента, попытки манипуляции и давления. Часто дети сталкиваются с такими угрозами раньше, чем успевают понять, как им противостоять, а взрослые не всегда знают, что именно происходит с ребенком в цифровом пространстве.

Мы убеждены: чтобы защитить детей в интернете, недостаточно только технологий. Важно понимать, как именно они живут онлайн, чему доверяют, чего боятся и с какими проблемами сталкиваются. Поэтому «Лаборатория Касперского» много лет подряд проводит опросы на тему цифровых привычек детей и родителей, а затем превращает полученные знания в практические решения — образовательные программы, полезные материалы и инициативы, доступные семьям, школам и сообществам в разных странах.

О чем говорят наши исследования?

Один из ключевых проектов Компании в области обеспечения цифровой безопасности детей — регулярное исследование, на основе которого мы готовим аналитический отчет [«Взрослые и дети в интернете»](#). В 2024 году в нем участвовали 2 026 респондентов из крупных городов России — 1 013 пар «родитель — ребенок» (дети от 3 до 17 лет). Опрос охватывал повседневную цифровую жизнь: использование соцсетей и онлайн-сервисов, игры, общение, а также столкновения с мошенничеством, кибербуллингом и небезопасным контентом.

Мы также изучаем, как злоумышленники используют популярность детских брендов. Так, в [отчетном периоде](#) наши эксперты проанализировали угрозы, использующие в качестве приманки упоминание известных игр, игрушек и мультфильмов (Minecraft, Roblox, LEGO, Disney и др.). Исследование показало, что только за первый квартал 2024 года число таких атак выросло на 35% по сравнению с годом ранее.

В 2025 году мы продолжили анализировать цифровые привычки детей, используя обезличенные данные решения [Kaspersky Safe Kids](#). Они показывают, что дети все больше времени проводят в онлайн-играх, видеоплатформах и социальных сервисах, чаще используют мобильные устройства и активно интересуются игровым и видеоконтентом.

При этом для них сохраняются ключевые риски — столкновения с мошенничеством, нежелательным контентом и попытками давления со стороны незнакомых пользователей. Эти данные подтверждают необходимость комплексного подхода к детской онлайн-безопасности, сочетающего технологическую защиту, обучение и развитие цифровой грамотности детей и родителей.

Результаты исследований

Основные тренды цифрового поведения детей в 2024–2025 годах

- 54% детей 3–6 лет регулярно используют смартфон.
- Почти 98% детей 11–14 лет имеют собственный смартфон, и большинство используют его ежедневно.
- Время, проведенное онлайн, увеличивается с возрастом: 56% старшеклассников ежедневно проводят в Сети три часа и более, а 20% говорят, что находятся онлайн практически все свободное время.
- В начале 2025 года дети чаще проводили время в мессенджерах и приложениях, представляющих короткие видео. В десятку лидеров по времени использования вошли Telegram, WhatsApp, TikTok и Roblox.
- В 2025 году интерес к чат-ботам на базе ИИ вырос более чем вдвое.

Обучаем и помогаем — детям, родителям и педагогам

Мы считаем, что процесс освоения цифровой грамотности должен быть доступным, понятным и интересным. Поэтому «Лаборатория Касперского» активно участвует в образовательных и просветительских проектах.

- **«Урок цифры».** В рамках федерального проекта «Урок цифры» в 2025 учебном году мы провели занятия по теме «Кибербезопасность и искусственный интеллект». Школьники, учителя и родители знакомились с базовыми правилами безопасного использования ИИ-технологий, учились распознавать онлайн-мошенничество и узнавали, как специалисты по кибербезопасности используют машинное обучение. Только за первые три недели интерактивные тренажеры были пройдены более **3,5 млн раз**.
- **«Цифровой ликбез».** Для нового сезона всероссийского просветительского проекта «Цифровой ликбез», реализуемого в рамках национального проекта «Экономика данных» и национальной цели «Технологическое лидерство», мы подготовили серию обучающих видеороликов для детей от шести лет. Один из них посвящен проблеме онлайн-груминга, другой — мошенничеству в популярных кликер-играх. Видео рекомендованы для совместного просмотра с родителями или педагогами и сопровождаются методическими материалами, которые можно использовать на уроках, во внеурочной деятельности и при работе с семьями.

Понятные материалы для всей семьи

Чтобы говорить о цифровой грамотности и других сложных вещах простым языком, мы создаем специальные издания для детей и взрослых.

- **«Киберазбука»** — познавательная книга о мире технологий и цифровых угроз, построенная по принципу алфавита. Она помогает детям и родителям разобраться в новых терминах и научиться безопасному поведению в Сети. В 2024–2025 годах мы перевели книгу на 15 языков, а в октябре 2024 года состоялся коммерческий релиз «Киберазбуки» на русском языке.
- **«Цифровой портфель»** — практическое пособие для родителей с советами о том, как защитить ребенка как в онлайн-, так и в офлайн-мире: от настройки устройств до бесед о безопасности и доверии. Руководство доступно бесплатно и ориентировано на родителей без технического бэкграунда.

Региональные инициативы

Наша работа по защите детей в интернете выходит далеко за пределы одной страны.

- В **Италии** в рамках Privacy Tour, организованного Итальянским агентством по защите данных, мы передали 500 экземпляров «Киберазбуки» участникам образовательных мероприятий.
- В **Германии** на крупнейшей отраслевой IT-выставке it-sa Expo&Congress в Нюрнберге участники получили 500 таких же книг.
- В **Марокко** наши эксперты приняли участие в семейном дне в школе Cadi Ayad в Касабланке, где рассказали детям и родителям о цифровых рисках и способах защиты от них, а также представили им «Киберазбуку». В мероприятии участвовали порядка 50 детей и их родителей.

KidZania — безопасность через игру и опыт

В марте 2025 года мы открыли [Центр киберисследований](#) в детском образовательном парке KidZania Santa Fe в Мексике. Здесь, в известном развлекательном городе, дети в игровой форме знакомятся с основами кибербезопасности, выполняют практические задания и учатся распознавать цифровые риски.



Наши планы на 2026–2027 годы

- Выпуск аналитических отчетов и обучающих материалов по детской онлайн-безопасности
- Участие в образовательных и просветительских проектах для повышения цифровой грамотности среди детей, родителей и педагогов
- Открытие новых центров киберисследований в детском образовательном парке KidZania в Индии и ОАЭ
- Развитие партнерств с международными правоохранительными организациями, коалициями и НКО, нацеленных на борьбу со stalkingом