



# Цифровое преследование в отношениях

## Отчет

---

---

Что такое стalkerское ПО  
и можно ли его распознать?

**kaspersky** BRING ON  
THE FUTURE

## Оглавление

Введение .....	03
Что такое сталкерское ПО и могут ли люди его распознать? .....	04
Различия по демографическим признакам .....	05
и знаниям о функциях ПО	
Цифровой мониторинг и согласие .....	06
Цифровое преследование – насколько серьезна проблема? .....	09
Личное и конфиденциальное. Какой информацией .....	10
люди готовы делиться с партнерами?	
Как люди реагируют, когда обнаруживают, .....	12
что на их устройстве установлено сталкерское ПО?	
Как защититься от цифрового преследования? .....	14
Об исследовании .....	16

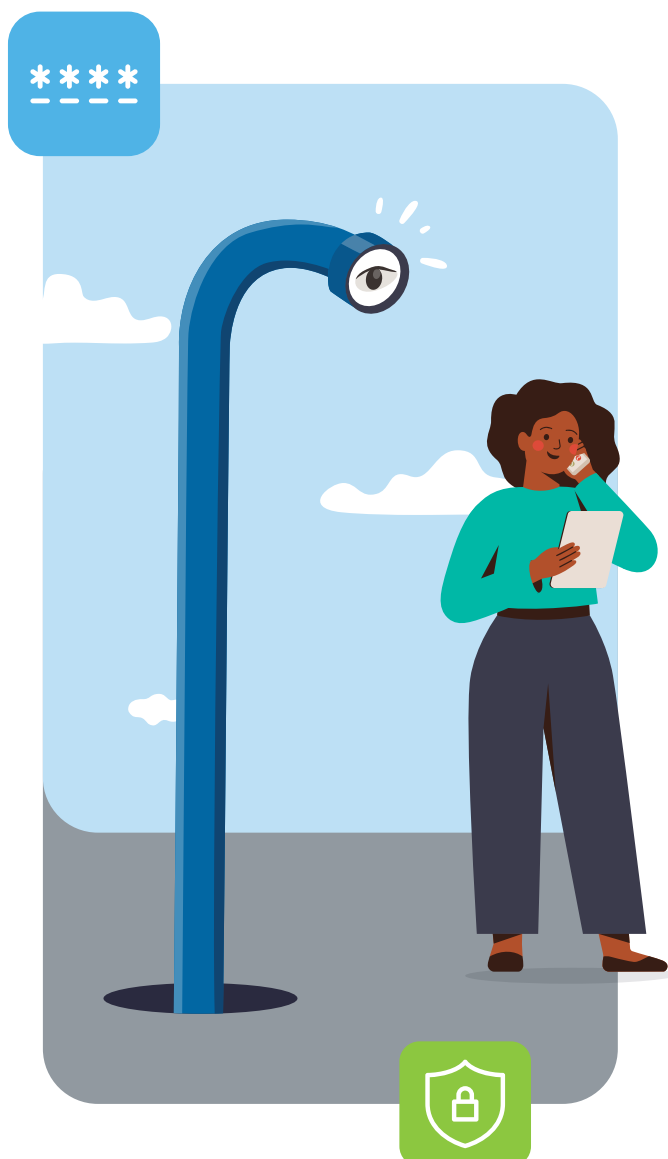


# Введение

В 2021 году поддерживать связь с людьми стало просто как никогда, во многом благодаря цифровым технологиям и умным устройствам, с помощью которых мы легко можем общаться по разным каналам связи. С одной стороны, у этого явления есть много положительных сторон: например, мы чувствуем поддержку близких несмотря на расстояние, становимся сплоченнее и быстрее заводим новые знакомства. С другой стороны, легкость доступа к нашим данным в сети может сыграть против нас.

При определённых обстоятельствах, цифровые технологии могут использоваться абьюзерами для нарушения приватности и совершения аморальных поступков. Существуют приложения, которые могут отслеживать местонахождение партнера, контролировать круг его общения и проверять историю посещенных веб-сайтов и прочую деятельность в интернете. Такие приложения называются сталкерскими.

В отчете анализируется исследование, проведенное компанией SAPIO по заказу «Лаборатории Касперского» и некоторых некоммерческих организаций, занимающихся вопросами домашнего насилия.



**Целью исследования было определить насколько широко распространено сталкерское ПО, которое также иногда называют spouseware, «ПО для слежки за партнером» и собрать данные, которые помогут специалистам по борьбе с домашним насилием глубже понять проблему и повысить качество помощи жертвам.**

## Задачи исследования:

- Выяснить, сколько людей знают о сталкерском ПО и его функциях
- Проанализировать, как и когда люди следят за своим партнером
- Понять, какими данными люди готовы делиться, а какие хотят хранить вдали от посторонних глаз
- Понять сколько людей, стало жертвами сталкерского ПО
- Понять, какими устройствами чаще всего пользуются абьюзеры для слежки за жертвами

**Наше исследование показало, что большинство людей не знают, что такое стalkerское ПО. 60% наших респондентов ответило именно так. Тем не менее, все же есть небольшая группа людей, которые знают для чего нужны подобные программы. Для России проблема также актуальна.**

## **Что такое стalkerское ПО и могут ли люди его распознать?**

Стalkerское ПО – это программное обеспечение, которое используется в том числе для слежки за своим партнером или другим близким человеком. Это коммерческие программы, которые устанавливаются на чужой смартфон. Для активации приложения злоумышленнику достаточно всего один раз получить физический доступ к устройству жертвы, а такая возможность у преследователя, как правило, есть: согласно исследованию, большинство людей доверяют своим партнерам и, как правило, могут предоставлять физический доступ к своим устройствам.



Пользоваться стalkerскими приложениями неэтично, но в некоторых странах их использование уже преследуется по закону. Часто их распространяют под видом решений для родительского контроля или защиты от кражи. Однако, сколько людей знает о существовании и доступности таких приложений? И об угрозах, которые они могут нести?

Наше исследование показало, что большинство людей не знают, что такое стalkerское ПО. 60% наших респондентов ответило именно так. Тем не менее, все же есть небольшая группа людей (40%), которые знают для чего нужны подобные программы. Можно предположить, что почти половина опрошенных либо сами пользовались подобными приложениями, либо стали жертвой преследователя, что звучит довольно пессимистично.

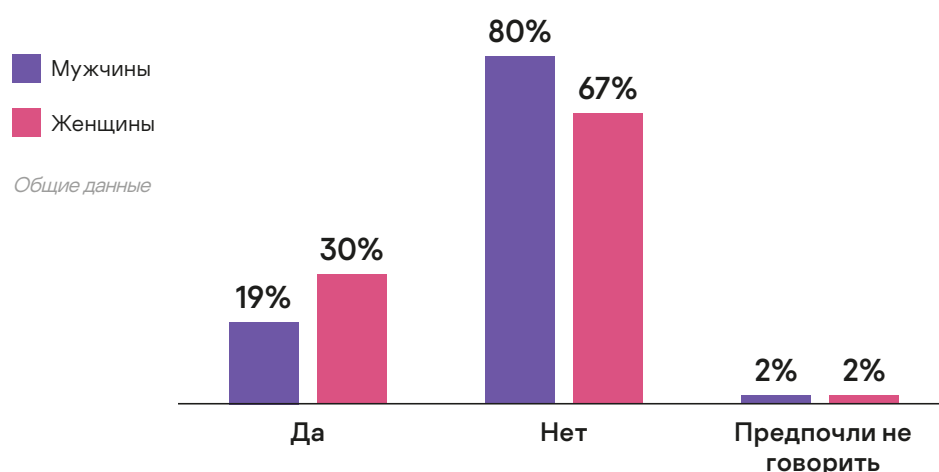
Однако совсем не обязательно познавать все на собственном опыте, для того, чтобы ознакомиться с чем-либо. К тому же название «стalkerское ПО» говорит само за себя. Не составит труда провести аналогию с другими шпионскими приложениями, чтобы понять, какую функцию оно выполняет. Даже самой общей информации о стalkerских программах достаточно, чтобы понять, что они достаточно распространены и от них могут пострадать тысячи людей. Нужно серьезно относиться к этой проблеме и принимать соответствующие меры для защиты конфиденциальности огромного количества людей.

В России 29% опрошенных респондентов ответили, что знают о существовании и функциях стalkerского ПО. Подобная статистика несколько лучше, чем в странах Европы и Латинской Америки (Франция – 49% ответили, что знают, Бразилия – 30% ответили, что знают) Однако нельзя игнорировать эту проблему, так как данные огромного количества пользователей находятся под угрозой.

# Различия по демографическим признакам и знаниям о функциях ПО

Существуют некоторые важные различия, о которых следует знать, когда речь идет об уровне осведомленности о стalkerских программах. Во-первых, больше мужчин (44%), чем женщин (36%), знают о существовании стalkerских программ. Во-вторых, молодые люди чаще осведомлены о преследовательских программах, чем респонденты старшего возраста: о них знают 46% людей в возрасте от 16 до 34 лет и только 28% опрошенных старше 55 лет.

## Вы когда нибудь сталкивались с насилием или жестоким обращением со стороны вашего партнера?



Подробный анализ данных позволяет выявить возможные причины таких различий. Больше мужчин (10%), чем женщин (8%), признались, что устанавливали мониторингающие программы на устройство своего партнера. А поскольку такие приложения незаметно работают в фоновом режиме, логично, что абьюзеры знают о них гораздо больше, чем жертвы. Этот вывод подкрепляется тем фактом, что женщины чаще, чем мужчины, становятся жертвами домашнего насилия со стороны своих партнеров (30% против 19%).

Что касается возрастных различий, люди в возрасте от 16 до 34 лет склонны подозревать своих партнеров в слежке гораздо чаще, чем опрошенные старше 55 лет (45% и 20%). Это может быть связано с тем, что молодые люди выросли и живут в среде, где доминируют цифровые технологии. Или же они более остро осознают возможность того, что их цифровая конфиденциальность может быть нарушена в результате использования стalkerского программного обеспечения.

Но даже среди тех, кто имел дело с программами, предназначенными для скрытого мониторинга, есть люди, которые знакомы с некоторыми функциями лучше других. Многие знают, что стalkerское ПО используется для мониторинга активности в интернете (72%), определения местоположения (68%), а также видео- и аудиозаписи (60%). Однако лишь 42% опрошенных знают, что преследователь может получать уведомления о попытках жертвы удалить приложение с устройства. Поэтому предстоит провести еще много просветительской работы в отношении стalkerского ПО и предупредить возможных жертв о его функциональных возможностях. При этом в первую очередь нужно ориентироваться на опасения и потребности самих жертв.

В России ситуация не сильно отличается от общемировой картины. Несмотря на то, что большая часть респондентов не знает о существовании стalkerского ПО, о функциях этого программного обеспечения догадываются многие. Так, 71% опрошенных граждан догадывается о том, что стalkerские программы позволяют мониторить активность жертвы в интернете, 53% уверены, что ПО позволяет отслеживать видео и аудиозаписи. Кроме того, только 31% пользователей знает о том, что абьюзер получит уведомление, если жертва постарается стереть приложение с устройства.

“Эрика Олсен (Erica Olsen), директор проекта Национальной сети по искоренению домашнего насилия (NNEDV), предупреждает: «Абьюзер может стать еще агрессивнее, если почувствует сопротивление или если жертва удалит ПО, с помощью которого он мониторил все ее действия. Жертвам следует выбрать самый безопасный для себя сценарий в данный момент и обратиться в службу помощи жертвам домашнего насилия за информацией о возможных вариантах действий».

## Цифровой мониторинг и согласие

В вопросе о сталкерском ПО (и программах для наблюдения в целом) нельзя не коснуться темы согласия. К счастью, подавляющее большинство опрошенных (70%) считают, что следить за партнером без его согласия недопустимо. Но даже оставшиеся 30% людей, которые уверены, что согласие партнера не требуется (по крайней мере, в некоторых ситуациях), – довольно тревожная статистика.

В России, к сожалению, куда более неутешительная статистика. Только 57% опрошенных граждан убеждены в том, что следить за партнером без взаимного согласия недопустимо. Кроме того, 15% респондентов не видят в слежке за партнёром без его согласия ничего плохого, а 28% уверены, что слежка допустима лишь при определенных обстоятельствах. Интересным является также тот факт, что 28% опрошенных граждан беспокоятся или беспокоились о том, что романтический партнер может нарушить их цифровую конфиденциальность.

### Можно ли следить за своим партнером без его ведома?





Эта цифра вызывает особую тревогу, так как позволяет предположить, что примерно 21% респондентов, которые подозревали, что их партнер шпионит за ними через подобное приложение, могут быть правы. Эксперты, работающие непосредственно с жертвами домашнего насилия, предполагали, что эта цифра ниже. Специалисты отмечают, что такого рода преследование часто прикрывают заботой о безопасности жертвы.

По данным опроса, почти две трети тех, кто считает, что согласие ни к чему, готовы следить за партнером, если заподозрят его в неверности (64%), если от этого будет зависеть его безопасность (63%) или если у них появятся основания полагать, что партнер замешан в какой-либо незаконной деятельности (50%). Слежка за партнером из-за подозрения в измене еще раз подтверждает агрессивный, насильственный характер использования стalkerского ПО. Как отмечает Берта Валл Кастелло (Berta Vall Castelló), директор по научно-исследовательской деятельности Европейской сети по работе с виновными в домашнем насилии (European Network for the Work with Perpetrators, WWP EN), такое подозрение нельзя считать уважительной причиной, несмотря на то, что огромное количество людей считают ее таковой.

В России главным основанием для слежки за партнером является забота о безопасности (63%), в то время как подозрения в неверности отошли на второй план (60%). Однако если основной причиной слежки являются благие намерения, то почему нельзя установить приложения с согласия партнера?

Кроме того, многие из опрошенных граждан не против делиться с партнером своими цифровыми данными. Своими фотографиями готовы поделиться 58% респондентов, доступ к социальным сетям готовы предоставить 45% опрошенных и 49% готовы поделиться списком контактов.

«Эти результаты позволяют говорить об идеализированной романтической любви, которую чаще всего испытывают подростки, – у них нет тайн от любимого человека, они готовы полностью открыться ему, демонстрируя так свои искренние чувства и доверие», – говорит Берта Валл Каstellо из Европейской сети по работе с виновными в домашнем насилии WWP-EN.



Беспокойство о своей половинке тоже вызывает немало вопросов. Если вы следите за партнером из соображений безопасности, то почему бы не сказать об этом прямо, не заручиться согласием и не позволить при желании удалить приложение? Что касается проверки причастности к преступлению, для этого существуют гораздо более очевидные и эффективные способы, чем использование приложений для слежки.

В некоторых странах люди сталкиваются с проблемой использования стalkerского ПО без согласия другой стороны гораздо чаще, чем в других. Индия (47%), Малайзия (32%) и Китай (23%) заняли самые высокие позиции в нашем рейтинге стран, жители которых готовы следить за своим партнером без их согласия. В других странах эта идея получила гораздо меньше поддержки: Португалия и Колумбия – 7%; Испания, Чехия, Мексика, Перу – 6%; Аргентина – 5%. Отчасти это может быть связано с культурными представлениями о праве на неприкосновенность частной жизни: в Индии менее четверти респондентов (24%) считает, что такое право есть у каждого, в то время как в Испании и Мексике этого мнения придерживаются 65% опрошенных.

В России 19% респондентов преследовались при помощи стalkerских ПО. Кроме того, 12% опрошенных подозревают своих партнеров в использовании стalkerского ПО.

Слежку за партнером с его согласия одобряют гораздо больше людей. Почти половина (48%) теоретически могла наблюдать за своим партнером по согласию: 25% в интересах «полной прозрачности» отношений, а оставшиеся 24% следили бы за партнером только при определенных обстоятельствах (если это нужно для обеспечения его физической безопасности или если такой мониторинг будет взаимным). В России слежку за партнером с его согласия одобряют 26% опрошенных граждан.

«Эти результаты позволяют говорить об идеализированной романтической любви, которую чаще всего испытывают подростки, – у них нет тайн от любимого человека, они готовы полностью открыться ему, демонстрируя так свои искренние чувства и доверие», – говорит Берта Валл Каstellо из Европейской сети по работе с виновными в домашнем насилии.



## Цифровое преследование – насколько серьезна проблема?

В двух словах, цифровое преследование – проблема довольно распространенная. Каждый четвертый (25%) подвергался насилию со стороны партнера в той или иной форме. В тоже время, мужчины становились жертвами реже (19%), чем женщины (30%). Самая распространенная форма насилия, с которой столкнулись 72% опрошенных, – психологическое насилие. От физического насилия пострадали 46%, а от финансового – 34%.

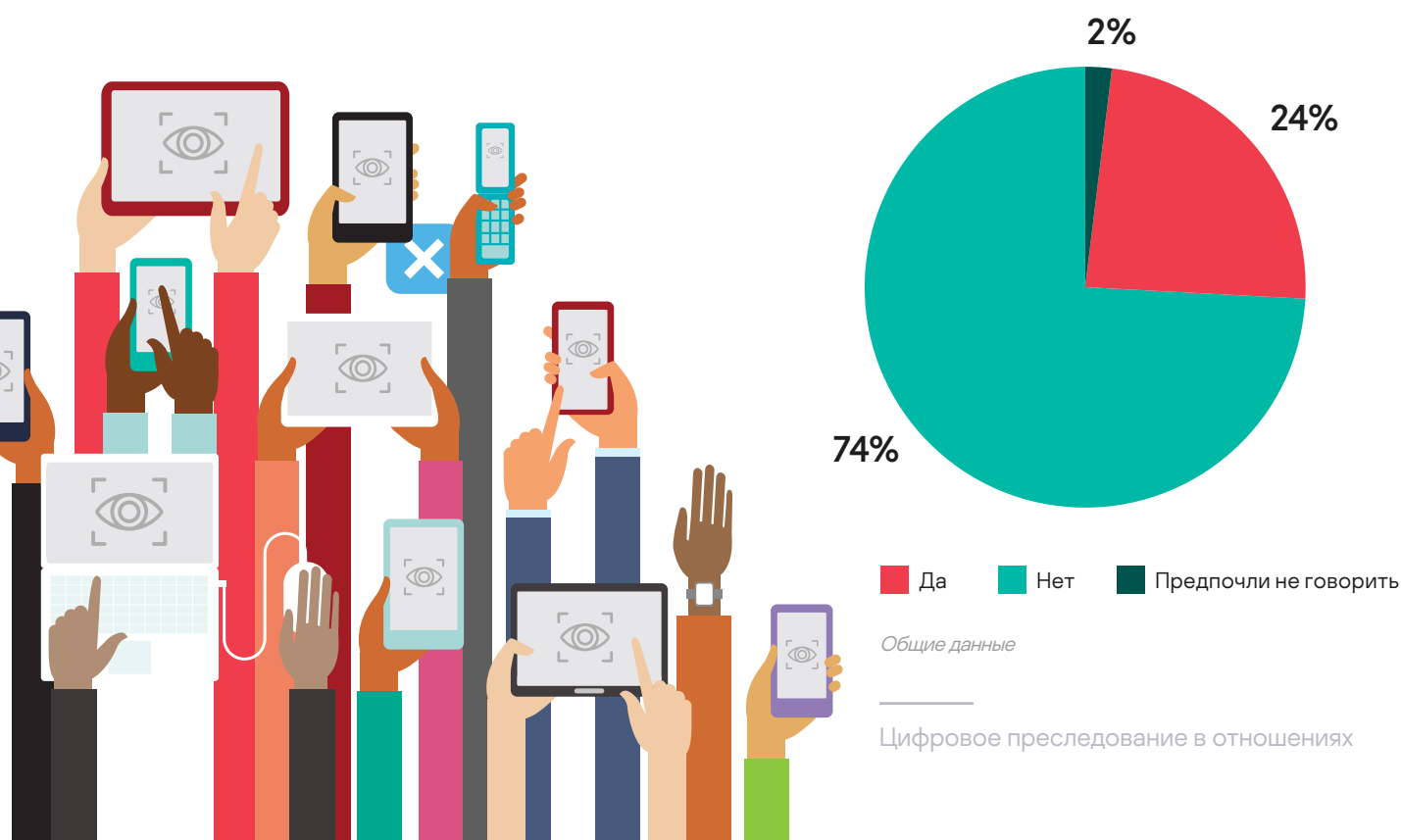
В России с насилием со стороны партнера так или иначе столкнулись 19% респондентов, из них с психологическим насилием столкнулся 61% опрошенных, а с физическим 58%. Данные свидетельствуют о том, что цифровое насилие, то есть слежка через стalkerские приложения – это может быть первым шагом на пути к психологическому насилию. Почти четверть респондентов (24%) уже стали жертвами цифрового преследования, а 37% только подозревают, что партнер следит за ними.

На наших смартфонах хранится много информации, и установка стalkerского ПО вызывает особые опасения за ее сохранность и конфиденциальность. Больше всего респондентов беспокоило, что партнер может получить доступ к их аккаунтам в соцсетях (53%), сообщениям (51%) и электронной почте (45%). И это довольно тревожная статистика, ведь за половиной респондентов, ставших жертвой преследователя, следили с помощью мобильного приложения (50%).

В некоторых регионах люди больше беспокоятся о своей конфиденциальности, чем в других. Более половины респондентов из Перу и Колумбии (56%) считают, что партнер следит за ними. При этом в Германии и Нидерландах так думают только 20% опрошенных. На это может быть несколько причин, в том числе разные культурные представления о конфиденциальности или о личной информации, которую можно хранить на цифровых устройствах, не скрывая от посторонних глаз.

Однако даже в странах, которые заняли последние строчки в нашем рейтинге, каждый пятый беспокоится о приватности своих данных и неприкосновенности частной жизни. Это значительное число, которое свидетельствует о наличии проблем, требующих решения.

### Вас когданибудь преследовали при помощи технологий?



## Личное и конфиденциальное. Какой информацией люди готовы делиться с партнерами?

Конфиденциальность – понятие неоднозначное. Каждый человек сам определяет, какой информацией он готов поделиться с партнером. Например, более половины респондентов (57%) давали партнеру пароль от своего мобильного, и примерно столько же (56%) знают пароль от смартфона партнера. Более 42% сообщали членам семьи данные для входа в свою учетную запись iCloud или Google. То есть многие люди не скрывают своей цифровой активности от партнеров или близких родственников.



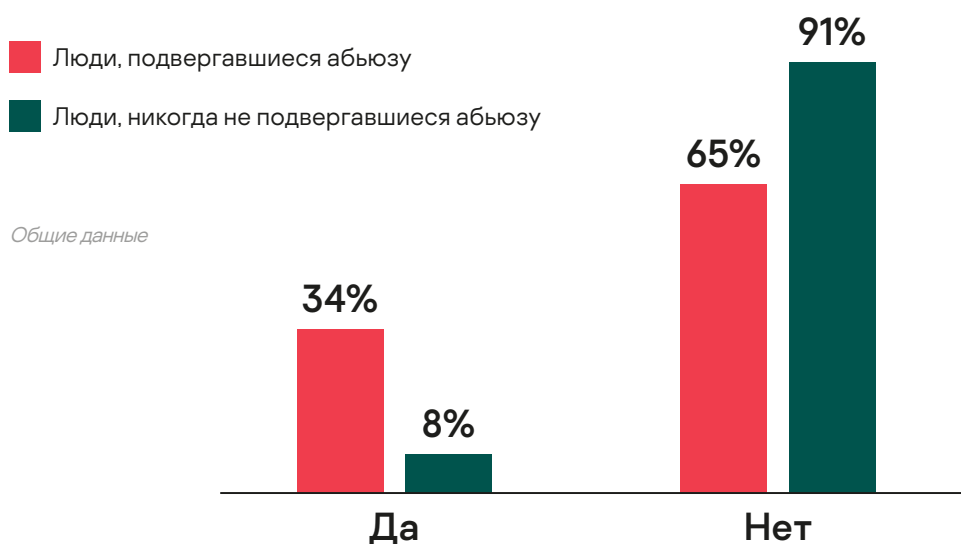
Но, опять же, происходит это с согласия пользователя, и ситуация скорее выигрышная для обеих сторон и свидетельствует о здоровых отношениях, а не о злоупотреблении доверием и слежке. Но одного лишь пароля недостаточно – для просмотра информации нужно получить физический доступ к устройству. Если у вас здоровые отношения и вы решили ограничить доступ партнера к своему устройству, то вы можете в любой момент перестать давать ему мобильный или поменять пароль.

Даже если вы готовы открыть ему доступ к своей цифровой жизни, всегда найдутся данные, которыми вам на самом деле не очень захочется делиться. Двое из пяти респондентов никому не говорят свой пароль (38%), четверть опрошенных никогда бы не поделились записью своих разговоров (26%), а 25% не готовы открывать партнеру финансовую информацию. При этом только 10% не намерены показывать партнеру свои фотографии, и только 17% не горят желанием давать доступ к своим аккаунтам в социальных сетях и камере.

## Практически каждый десятый (9%) признал, что устанавливал мониторинжные приложения на смартфон партнера, и еще 9% использовали функции умного дома, чтобы следить за своей второй половиной без ее согласия»

Сталкерское ПО процветает именно в тех обстоятельствах, когда существует дисбаланс между уровнем доступа к информации, которую хочет получить один партнер и которую не хочет раскрывать другой: 15% опрошенных отметили, что партнер просил их установить приложение для мониторинга, из них жертвой насилия стали 34%, что несравнимо больше тех, кого это миновало (8%). Пожалуй, это самое убедительное доказательство того, что между использованием сталкерского ПО и абьюзом есть прямая связь.

### Требовал ли когда либо ваш партнер установить приложение для слежки?



Людей в возрасте от 18 до 34 лет установить приложение с функцией полного мониторинга просили гораздо чаще, чем лиц старше 55 лет (21% и 5% соответственно). Это позволяет сделать еще один важный вывод: использование сталкерского ПО сопряжено с абьюзом и молодое поколение может быть больше подвержено пагубным последствиям.

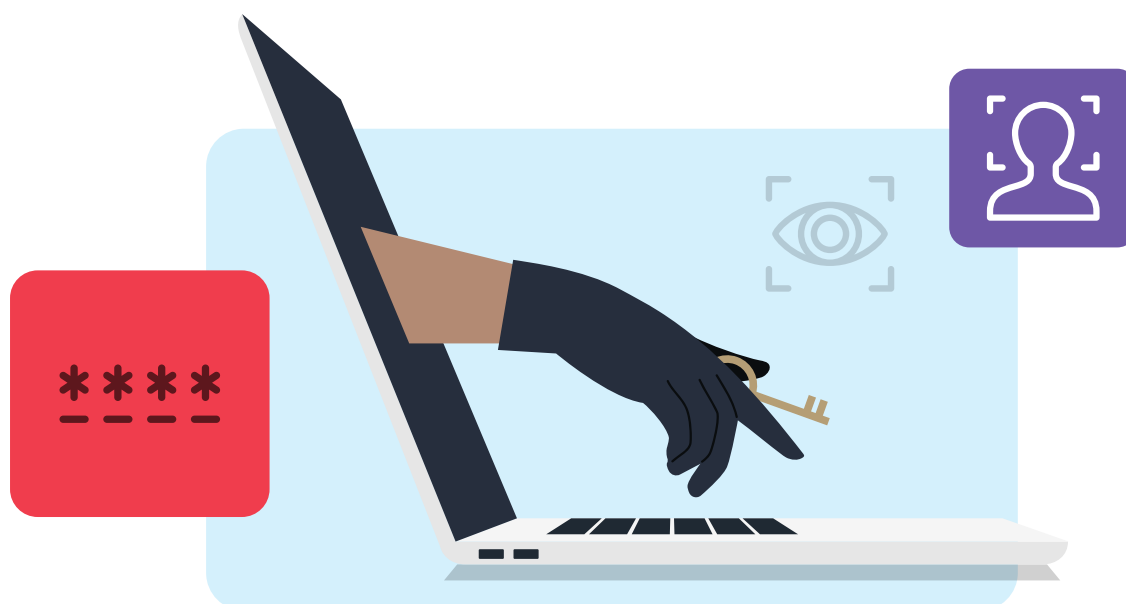
Большинство респондентов, принявших участие в опросе (84%), не разрешают партнерам устанавливать программы и менять настройки на их телефоне. Однако в разных регионах мнения по этому поводу расходятся. Например, в Индии более трети респондентов (38%) сказали, что их партнер устанавливает приложения или меняет параметры на их смартфоне, а в Австралии положительно ответили на этот вопрос лишь 7% опрошенных.

Количество людей, которые продолжают нарушать личные границы и пытаются любой ценой получить доступ к конфиденциальной информации своих близких (по крайней мере, не спрашивают об этом), довольно велико: каждый десятый (9%) признал, что устанавливал приложения для скрытого мониторинга на смартфон партнера, и еще 9% использовали функции умного дома, чтобы следить за своей второй половиной без ее согласия.

## Как люди реагируют, когда видят стalkerское ПО на своем устройстве?

Те, кто стал жертвой абьюзера или только подозревают, что за ними следят, реагируют абсолютно по-разному. Это вполне объяснимо, ведь уникальна каждая ситуация, в которой люди понимают, что они уязвимы: личные обстоятельства, доступные каналы поддержки, сложившиеся в обществе понятия о насилии и особенности отношений.

Около половины (50%) опрошенных готовы найти того, кто установил мониторящее ПО на их устройство, и потребовать объяснений у абьюзера лично. В России число людей, которые ответили так же, тоже составляет 50%. Большинство респондентов (83%) хотели бы серьезно поговорить с партнером, если бы обнаружили на своем телефоне подобное приложение, установленное без их согласия. Однако в этом случае выяснение отношений может лишь усугубить ситуацию, и эксперты, работающие с жертвами домашнего насилия, настоятельно не рекомендуют этого делать. Это еще раз подчеркивает необходимость работы по подготовке, обучению и поддержке людей в сложных ситуациях, связанных с преследованием.



Только 17% респондентов готовы позвонить по телефону горячей линии или лично обратиться в центр поддержки в такой ситуации. В России число еще ниже и составляет 14%. В Европе число таких людей может составлять всего 12%. Это может быть связано с тем, что многие не считают стalkerское ПО серьезной угрозой, сопряженной с домашним насилием, или не имеют четкого представления о том, какую поддержку можно получить в специализированных службах.

**«Жертвы домашнего насилия, которые пытаются противостоять партнеру, установившему стalkerское ПО на их мобильное устройство, могут подвергнуть себя еще большему риску. Нас беспокоит то, что позвонить по телефону горячей линии или лично обратиться в центр поддержки готовы так мало респондентов. В случае насильственного контроля со стороны партнера крайне важно получить поддержку специалиста и действовать согласно разработанному экспертами плану безопасности, чтобы снизить дальнейшие риски», – советует Берта Валл Каstellо.**



Среди тех, кто не стал бы выяснять отношений с партнером, обнаружив на своем смартфоне подобного мобильного шпиона, 26% не стали бы этого делать, потому что, по их мнению, разговорами проблему не решить, 24% – потому, что у них нет доказательств причастности партнера к этому, и 24% – потому, что будут искать другой выход из ситуации. Такие мотивы говорят о нездоровых отношениях, в которых существует серьезный риск повышения агрессии партнера.

Если один из партнеров не может четко обозначить другому свои личные границы, скорее всего, он боится, что это приведет к неприятностям. Даже если, по их мнению, разговор ничего не решит, совершенно очевидно, что партнер не придает особого значения их независимости и интересам. Специалисты рекомендуют искать другой выход из ситуации, особенно если пострадавшая сторона всерьез обеспокоена собственной безопасностью. Но что именно делать?

### Какие технологии использовались для вашего преследования?



---

«Если использование сталкерского ПО сопряжено с домашним насилием или жестокостью, возможно, абьюзер намерен жестко контролировать своего партнера и может стать еще агрессивнее. Я настоятельно рекомендую обратиться за помощью в организацию, которая оказывает поддержку жертвам домашнего насилия, если вы столкнулись с преследованием – физическим или цифровым – и чувствуете, что противостоять партнеру опасно, – говорит Карен Бентли, глава **WESNET** и эксперт по технологиям безопасности. – [В рамках проекта по борьбе с домашним насилием](#) под руководством организаций NNEDV в США и **WESNET** в Австралии доступны инструменты, обеспечивающие онлайн-безопасность и защиту конфиденциальности и позволяющие жертвам домашнего насилия получить консультацию по поводу шпионского ПО», – добавляет она.



## Как защититься от цифрового преследования?

Исследование показало, что сталкерское ПО – проблема неприятная и даже опасная. Как узнать, что за вами следят? Несмотря на то что сталкерские программы работают незаметно, большинство из них все же так или иначе проявляют себя. Вам следует насторожиться, если на устройстве увеличился объем исходящего мобильного трафика или батарея садится слишком быстро. Проверьте, какие приложения потребляют ресурсы смартфона.

Кроме того, проверьте все ПО, которые использует данные о вашем местоположении. Если на устройстве Android вы не обнаружили ничего подозрительного, но уверены, что за вами следят, поищите приложения, которые используют специальные возможности (найдите раздел «Специальные возможности» в настройках).

Они позволяют приложениям вмешиваться в работу остальных программ, менять настройки и совершать много других действий от имени пользователя, делая устройство уязвимым к сталкерскому ПО. Доступ Android-приложений к специальным возможностям – может быть одним из самых опасных разрешений, и мы рекомендуем давать его только антивирусной программе.

---

**Защитите устройство сложным паролем и не сообщайте его ни партнеру, ни друзьям, ни коллегам. Никому.**



Есть и другие способы обнаружить такого мобильного шпиона, например установить приложения Kaspersky Internet Security для Android или TinyCheck (Последнее – только под контролем экспертов). [Здесь](#) можно найти подробные инструкции. Если вам удалось обнаружить стalkerское приложение на своем смартфоне, не спешите удалять его. Тот, кто установил программу, это заметит и может стать еще агрессивнее. К тому же вместе с приложением вы удалите и улики, которые могут понадобиться вам в дальнейшем.

Как и в любой другой ситуации, угрожающей вашей безопасности сначала подумайте, как защитить себя от возможных неприятностей. Например, если человек, который следит за вами, потенциально опасен, обратитесь в центр поддержки пострадавших от домашнего насилия, прежде чем принимать какие-то меры (подробнее см. [здесь](#)).

**В некоторых случаях проще заменить смартфон и следить за тем, чтобы никто не устанавливал нежелательных программ на новое устройство. Тогда как для предотвращения угрозы следуйте советам «Лаборатории Касперского»:**

- Защитите устройство сложным паролем и не сообщайте его ни партнеру, ни друзьям, ни коллегам.
- Поменяйте пароли от всех аккаунтов.
- Скачивайте приложения только из официальных магазинов, например из Google Play или App Store.
- Сразу же установите [надежное защитное решение](#) и регулярно проверяйте устройство. Делайте это только после оценки потенциальных рисков, поскольку абыззер может заметить, что вы используете решение кибербезопасности.
- Не спешите удалять стalkerское приложение – агрессор это узнает. Имейте в виду, что этот человек может представлять для вас опасность. Он может ответить действиями, которые приведут к неприятным для вас последствиям.
- Обратитесь за помощью в местные органы власти и организации, оказывающие поддержку жертвам домашнего насилия, и составьте безопасный план действий. Список таких организаций для разных стран можно найти на сайте [www.stopstalkerware.org](http://www.stopstalkerware.org).

Подробнее о стalkerских приложениях и о том, как с ними бороться, можно узнать на сайте [Coalition Against Stalkerware \(коалиции против стalkerского ПО\)](#), которая противодействует цифровому преследованию и домашнему насилию.

## Об исследовании

В ходе исследования мы опросили 21 055 человек из 21 страны, которые состоят или состояли в отношениях.

В России в исследовании приняло участие 1002 респондента.

Максимальная статистическая погрешность составляет 0,7%, доверительная вероятность – 95%, доля признака – 50%.

Исследование проводилось онлайн компанией Sapio Research в сентябре 2021 года методом опроса по электронной почте и онлайн-опроса.



Audience | Brand | Content Research



# Цифровое преследование в отношениях

## Отчет

---