

ИНФОРМАЦИОННЫЙ МИР: прятки по-новому



Диана Александровна Богданова,
старший научный сотрудник Института проблем
информатики Федерального исследовательского центра
«Информатика и управление» Российской академии наук,
кандидат педагогических наук

Далеко не всё, что встречается онлайн, представляет собой зло, и не каждое приложение, появляющееся на рынке, таит в себе опасность. Но, пытаясь уследить за занятиями подростков и детей в Интернете, следует не забывать о том, что, хотя приложения по своим первоначальным целям не представляют никакой угрозы, они нередко предоставляют детям возможность или подталкивают их сделать неправильный, плохой выбор.

• приложения • фотосообщения • тайный чат • секстинг • небезопасные действия

Рассмотрим некоторые приложения, которые могут нести потенциальную опасность.

1. Audio Manager. Вспоминая детские загадки, например, «Сидит дед, во 100 шуб одет.....» или «Девушка в темнице, а коса на улице», мы понимаем, что речь на самом деле идёт и не о девушке, и не о деде. Так же следует относиться к названию приложения и в этом случае. Audio Manager не имеет отношения ни к проигрыванию музыкальных файлов, ни регулированию громкости. Это одно из самых распространённых приложений, позволяющих скрывать то, что не должно быть увидено: это могут быть и другие приложения, и фотографии обнажённых, и тайная переписка, и видео. Чтобы их увидеть, нужно лишь нажать на экран подольше, тогда

экранная защита отомкнётся
[<https://trashbox.ru/link/hide-it-pro-ili-audio-manager-android/>].

2. Calculator%. Здесь, по сути, та же самая ситуация, правда, на экране появляется изображение калькулятора, и всё выглядит как настоящий калькулятор. Но стоит нажать на кнопку приложения — и можно будет увидеть неподобающие фотографии. Известно, что в прошлом году с первых полос газет не сходила информация об обнаружении в одной из школ Колорадо (США) группы из примерно 100 учащихся, занимавшихся секстингом, а по сути, распространением непристойных фотографий обнажённых учеников школы, младшему из которых было чуть более 10 лет. Поскольку во многих штатах очень строгое законодательство, в том

числе и в Калифорнии, и секстинг приравнивается к распространению порнографии, некоторым старшеклассникам грозит уголовное преследование, не говоря о внесении в национальную базу данных преступников, занимающихся распространением детской порнографии. И заниматься распространением учащиеся смогли, пользуясь этим приложением: оно скрывало всё содержание от посторонних глаз [<https://itunes.apple.com/us/app/private-photo-calculator-hide/id571206791?mt=8>].

3. Vaulty. Это приложение не только спрячет всё от бдительного родительского ока, но ещё и тайно сфотографирует и зафиксирует GPS-координаты того, кто попытается вскрыть приложение, не зная пароля. Приложение имеет дополнительную опцию ложного пароля, которая запускает другую подборку фотографий. Родителям, обнаружившим подобную вещь, останется только признать, что ребёнок что-то от них скрывает, и сделать соответствующие выводы. <https://play.google.com/store/apps/details?id=com.theronrogers.vaultyfree>].

4. Snapchat — довольно известное увлечение последнего времени, захватившее молодёжь: это управляемая передача фотосообщений — приложение для смартфонов. Владелец смартфона может снять фото или видео, снабдить его текстом и отправить адресату, указав при этом время, через которое это послание исчезнет из телефона получателя. Спустя заданное время фото действительно как бы исчезает навсегда. Этот сервис произвёл буквально революцию среди 13–25-летних, пересылая, по данным службы Snapchat, около 50 миллионов снимков ежедневно, позволяя таким образом «безопасно» обмениваться временами смешными, а временами — непристойными «посланиями». Дети фотографируются в классе, сидя в одиночестве или с друзьями. Основная цель этого сервиса — веселье, шутки. Но дети начали использовать этот сервис и для неприличных посланий, не задумываясь о возможных рисках. Сейчас его нередко используют для размещения на порносайтах так называемой «порнографии

места». Отправляя фривольную фотографию своему однокласснику, отправительница уверена, что в этом нет никакого риска, и фотография исчезнет с экрана спустя заданное время, однако потом эта фотография может оказаться на порносайте или будет иметь хождение среди одноклассников. Отправка обнажённых фото приняла в последние годы характер эпидемии, так что Snapchat safety center вынужден был напомнить своим пользователям, что обнажённые фотографии запрещены [<https://www.snapchat.com/>].

5. Burn Note так же, как и Snapchat, удаляет сообщения спустя некоторое время. Но, в отличие от Snapchat, с помощью Burn Note можно опрашивать только текстовые сообщения. А особенная черта этого приложения состоит в том, что оно показывает сообщение по одному слову, придавая сообщениям дополнительный оттенок секретности. Возможность удаления сообщения даёт детям ощущение дополнительного комфорта, хотя так же, как и в Snapchat, существует возможность продлить жизнь сообщения за счёт специальных мер. Это приложение, в силу возможности удаления сообщения, может использоваться для буллинга, поскольку даёт иллюзию безопасности для того, кто этим занимается [<https://burnnote.com/>].

6. Line — это настоящий мобильный хаб для чата, обмена фото и видео, обмена текстовыми сообщениями и видеозвонками. Однако «дьявол кроется в деталях». Приложение предлагает возможность тайного чата. Пользователи могут определить продолжительность существования сообщений (от двух секунд до недели). Кроме того, существует возможность пользования дополнительными функциями, что создаёт серьёзную опасность для родительского кошелька, если ребёнок знает пин код родительской кредитной карты. И хотя приложение объявляет, что дети должны получить разрешение родителей на пользование дополнительными возможностями, на самом деле никто ничего не проверяет [line.me/ru/].

7. Omegle даёт пользователям возможность онлайнного общения со случайными незнакомцами (что повторяет идею Chatroulette, о чём будет сказано далее). Анонимный чат на любые темы выглядит несколько пугающе: может быть чреват переходом к обсуждению сексуальных моментов, использованию непристойного языка или разговору на тему наркотиков, алкоголя и насилия. Некоторые собеседники сразу же спрашивают персональные данные, например, и адрес, возраст, пол и иную информацию, которую дети могут сообщить по неосторожности. В английском языке ASL (возраст, секс, место жительства) это устойчивая аббревиатура, используемая в сетевом общении. Детей следует держать от этого приложения как можно дальше [www.omegle.com].

8. Blendr использует для общения 300 миллионов своих пользователей возможности GPS навигации. Есть возможность обмениваться сообщениями, фото и видео и оценивать «крутизну» других пользователей. Поскольку не предусматривается аутентификация пользователей, сексуальные преступники беспрепятственно могут знакомиться с детьми и наоборот — и конечно, в приложении присутствует секстинг [blendr.com].

9. KiK — это сервис мгновенного обмена сообщениями, позволяющий обмениваться видео, фото и рисунками. Пользователи могут также создавать виртуальные подарки. Вроде бы всё выглядит очень пристойно. Однако, к сожалению, термин «KiK-приятель (KiK-buddy)» был со временем вытеснен другим: «секст-приятель». KiK не предусматривает аутентификации пользователей, а также родительского контроля, поэтому преступникам очень просто пользоваться приложением для того, чтобы завязывать контакты с детьми. А дети, получив анонимное имя, перемещаются на сайт типа Reddit и оставляют там своё имя, полученное на KiK [<http://www.kik.com/>].

10. Yik Yak. Это приложение можно назвать гибридом Twitter и Reddit с использованием GPS возможностей. Приложение даёт возможность отправлять только текстовые сообщения до 200 символов. Сообщения смогут прочитать 500 пользователей, которые ближе всего по GPS координатам будут находиться к автору сообщения. Проблема состоит в том, что поль-

зователи регулярно «подвергаются» рассылкам материалов сексуального характера, содержащим сквернословие, иногда и личные выпады от анонимных отправителей. Иногда этот сервис используется и для отправки сообщений с угрозами о заминировании учебного заведения. Девушка-подросток из Атланты после неудавшейся попытки суицида получила через Yik Yak сообщение с советом продолжать попытки. Скрываясь за завесой анонимности, пользователи не несут никакой ответственности за свои посты, занимаются распространением слухов и рассылкой угроз, культивируя, таким образом, зло [<https://www.yikyak.com>].

11. Ask.fm — один из самых популярных молодёжных сайтов, которым преимущественно пользуются дети. В разделе «Вопросы и ответы» пользователи могут анонимно задавать вопросы. Проблема состоит в том, что дети могут иногда намеренно выбрать одну жертву. Это — кибербуллинг без опасности быть разоблачённым. Этот сайт также известен девятию зарегистрированными фактами суицида. Последний, произошедший в 2013 году, открыл психологам явление «самобуллинга», когда ребёнок намеренно пишет о себе гадости в надежде, что кто-то за него вступится. Открытие произошло в результате расследования смерти 14-летней Анны Смит из местечка Люттеруорс (Великобритания). Убитый горем отец написал в Facebook, что нашёл буллинговые посты на странице своей дочери в ask.fm с пожеланиями смерти. Проведённое расследование показало, что посты писала сама девочка. Возникли предположения, что это форма нового тысячелетия вести дневник или писать стихи, выражая беспокойство и неуверенность. Или это сигнал семье и друзьям, что что-то идёт не так. Теперь, размещая страдание онлайн, подросток, испытывающий к себе ненависть, получает аудиторию. И, по мнению психиатров, занимающихся психологией подростков и проблемами, связанными с их зависимостью от технологий, пример, кажущийся единичным,

имеет гораздо более широкое распространение, чем это кажется. Специалисты отмечают, что незначительное число страдальцев, возможно, признали бы, что сами троллили себя онлайн. Новые владельцы сайта пообещали устранить буллинг или закрыть сайт совсем. Из произошедших изменений, известных автору, сайт стал модерируемым [<https://ask.fm/>].

12. Chatroulette. Сайт был разработан московским школьником Андреем Терновским. Его название возникло после просмотра фильма о вьетнамской войне, где герои фильма — заключённые играли в русскую рулетку. Главное его направление — общение между людьми всей планеты на основе вебкамеры, микрофона или просто текстовых сообщений с помощью клавиатуры. Люди соединяются случайным образом, выбор происходит среди подписчиков сайта. Первоначальная идея и быстрый рост популярности — от 500 визитов в день в течение первого месяца до 50 000 через месяц привели к 35 000 человек, связывающимся напрямую в каждый момент времени. Однако созданный с добрыми намерениями сайт начал использоваться отдельными посетителями с неблагоприятными целями. Один примерно из восьми участников соединения представлял обнажённым, демонстрируя себя либо своё участие в сексуальном акте. Университет Колорадо даже разработал программу, позволяющую различать лицо, глаза, кожу. А на следующем шаге программа определяет, не ведёт ли себя пользователь перед камерой ненадлежащим образом, и позволяет блокировать изображение. Любопытно, что для решения этой проблемы потребовались специальные технологии, не известные ранее: анализ движущегося изображения, полученного с вебкамеры. Ранее существовавшие программы работали со статичными изображениями высокого разрешения. Первоначальная результативность распознавания составляет примерно 60%. Продолжается совершенствование алгоритма, и его недостатки пытаются компенсировать модераторы [chatroulette.msk.ru].

13. Skout рекламирует себя как приложение, помогающее новым людям познакомиться и встретиться. Приложение оценивает приблизительно GPS координаты пользователя и со-

единяет его с другими людьми поблизости, давая возможность общаться и обмениваться виртуальными подарками. Прежде чем начать общение, приложение даёт возможность посмотреть на профили друга друга. У приложения есть интересная опция «потряси свой телефон», когда в результате произведённой «встряски телефона» приложение соединит случайным образом с другим пользователем, который тоже трясёт свой телефон. Соединившись, они могут анонимно общаться около минуты, прежде чем проявится профиль собеседника. За этим приложением есть отрицательная статистика инцидентов, произошедших в 2013 году, когда взрослые мужчины выдавали себя за детей и встречались со своими жертвами. В настоящее время, если пользователь не достиг 17-летнего возраста, приложение не будет соединять его с другими, находящимися ближе 100 миль. Но проверить корректность указанного возраста приложение не может, и руководство приложения не берётся гарантировать ничьей безопасности [www.skout.com].

Этот перечень приложений и сайтов, относительно которых родителям желательно быть в курсе, не претендует на полноту. Это просто напоминание о том, что много новых продуктов, позволяющих минимизировать или свести к нулю родительский контроль занятий детей в Сети, появляется на рынке. Если принять подход, принятый в семьях руководителей¹ и сотрудников² Кремниевой Долины, детей следует держать в стороне от технологий как можно дольше, регламентируя пользование лишь допустимым минимумом. Если придерживаться по отношению к технологиям более либерального взгляда, тем не менее, необходимо контролировать занятия ребёнка онлайн, проводить профилактические беседы или беседы уже по случаю обнаружения его небезопасных действий. **НО**

¹ Богданова Д.А. Электронная или печатная? // Дистанционное и виртуальное обучение. — 2013. — № 3. — С. 63–71.

² Богданова Д.А. Ещё раз о медиаграмотности и интернет-безопасности / Дистанционное и виртуальное обучение. — 2016. — № 5. — С. 74–82.