

Д. А. Богданова,

Федеральный исследовательский центр «Информатика и управление» Российской академии наук, г. Москва

ФОРУМ ЕВРОСОЮЗА ПО ДЕТСКОЙ ИНТЕРНЕТ-БЕЗОПАСНОСТИ SIF 2018

Аннотация

В статье представлен обзор мероприятий форума Евросоюза, посвященного вопросам детской интернет-безопасности Safer Internet Forum (SIF) 2018, который состоялся в Брюсселе, Бельгия, в ноябре 2018 года. Описаны рассмотренные на форуме актуальные интернет-риски, которым подвергаются пользователи Всемирной паутины, особенно дети.

Ключевые слова: самоидентификация, социализация, дипфейк, deepfake, персональные данные, онлайн-оффлайновая дихотомия, datadating brokers.

DOI: 10.32517/2221-1993-2018-17-9-7-9

Контактная информация

Богданова Диана Александровна, канд. пед. наук, ст. научный сотрудник Института кибернетики и образовательной информатики Федерального исследовательского центра «Информатика и управление» Российской академии наук, г. Москва; адрес: 119333, г. Москва, ул. Вавилова, д. 44, корп. 2; телефон: (499) 135-62-60; e-mail: d. a.bogdanova@mail.ru

D. A. Bogdanova,

Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow

THE EUROPEAN UNION FORUM ON KIDS' SAFETY IN INTERNET SIF 2018

Abstract

The article provides an overview of the activities of the European Union Forum on kids' safety in Internet Safer Internet Forum (SIF) 2018, which was held in Brussels, Belgium, in November 2018. The current Internet risks addressed by the World Wide Web users, especially children, are described.

Keywords: self-identification, socialization, deepfake, personal data, online offline dichotomy, datadating brokers.

В ноябре 2018 года в Брюсселе, Бельгия, состоялся ежегодный форум государств Евросоюза, посвященный вопросам детской интернет-безопасности [4]. Форум SIF (Safer Internet Forum) является ключевой ежегодной международной конференцией в Европе, на которой политики, исследователи, представители правоохранительных органов, молодежь, родители и воспитатели, преподаватели, представители промышленности, эксперты и другие участники встречаются для обсуждения последних тенденций, рисков и решений, связанных с безопасностью детей в интернете.

В этом году все мероприятия форума проходили под **общей темой «Влияние технологий на детей, молодежь и общество»**. Помимо участников из государств Евросоюза, а также из России, Армении, Украины в работе форума приняли участие специалисты из Нигерии, Марокко, Пакистана, Танзании, Албании, всего около 200 человек. На форуме 2018 года не было запланировано отдельных заседаний родителей-активистов, но традиционно была представлена довольно многочисленной группой молодежь, и для них была организована отдельная секция.

Программа форума включала пленарное заседание, церемонию награждения победителей конкурса образовательных ресурсов по интернет-безопасности, шесть секционных сессий и заключительную, итоговую, сессию.

Секционные заседания были посвящены обсуждению таких актуальных вопросов, как влияние технологии на самоидентификацию и личные отношения (включая некоторые реальные случаи), молодежные инициативы, проблемы и решения вокруг секстинга, логистика приема и обработки сообщений о противозаконном контенте в борьбе с сексуальной эксплуатацией детей. Каждый участник форума мог помимо пленарных заседаний посетить две секции на выбор. Все секции проходили дважды. Представленный в статье материал посвящен обзору тех заседаний, в работе которых приняла участие автор.

Форум открыл **пленарный доклад профессора психологии Линды Пападопулос (Linda Papadopoulou)**, в котором основное внимание было уделено влиянию технологий на самоидентификацию и формирование личных отношений. Профессор рассмотрела, как цифровые технологии трансформируют наше восприятие себя и наши отношения с другими.

Увеличивается понимание и признание того, что платформы, приложения и службы, которыми мы пользуемся, создавались не для того, чтобы помочь пользователям выразить себя, поддержать общение с другими, а *с целью извлечения прибыли*. И для этого разработчики данных сервисов делают все возможное, чтобы удержать пользователей, в частности детей, «на крючке». Показателем успеха каждой новой разработки является способность удерживать ребенка у компьютера как можно дольше. Из чего исходят разработчики:

- дети нуждаются в одобрении;
- они стремятся овладеть навыками;
- они хотят получить признание и ощущать себя частью группы.

Поэтому пользование продуктом должно быть максимально простым, пользователи необходимо стимулировать и напоминать ему о продукте. И платформы добиваются поставленных целей настолько успешно, что дети получают удовлетворение от общения с гаджетами гораздо большее, чем от потенциальных возможностей реального мира.

Каким образом компании добиваются этого?

Если речь идет об играх:

- игра дает детям чувство, что они являются мастерами в каком-то деле (чувство мастерства);
- дофамин — гормон радости, вырабатываемый организмом в процессе игры, — способствует формированию и закреплению привычек;

- еще совсем недавно перед разработчиками не стояла задача удерживать ребенка у компьютера как можно дольше; сегодня именно здесь происходят изменения;
- если успех игры зависит от времени, проведенного у компьютера, а не от времени, потраченного хорошо, — в этом случае создание принудительных игровых петель является неизбежным.

Если речь идет о социальных сетях, то здесь важны моменты социализации:

- потребность детей в социальном признании и боязнь отторжения по-прежнему остаются неизменными, но в социальных группах в режиме онлайн это выглядит иначе;
- подростки, естественно, стремятся к признанию сверстников, и это стремление возникает именно в том возрасте, когда они начинают использовать социальный инструмент, который предоставляют платформы (например, получение «лайков»);
- как и в играх, используются приемы психологии, направленные на удержание детей на социальных платформах;
- детей окружает новый набор элементов, о которых нужно беспокоиться, так как ребята уже усвоили, что есть социальная валюта, которая видна всем. Поэтому забота о продвижении себя не дает им отдохнуть от беспокойства о том, какими их видят другие.

Что могут сделать взрослые? Как они обеспечат безопасное путешествие во Всемирной паутине для детей, осваивающих новый цифровой мир, чего им, взрослым, делать никогда не приходилось? Здесь роль родителей и сложность вызовов, стоящих перед ними, трудно переоценить. Это необходимость бесед с детьми, необходимость установления регулирующих ограничений, воспитание сознательности — все тот же стандартный набор рекомендаций для родителей, но адаптированный к условиям меняющейся среды, в которой проводят время и взрослеют дети.

Первое секционное заседание было посвящено дипфейкам (**deepfake**). Что это за новый термин — **deepfake**? Он образован комбинацией двух терминов — **deep learning** и **fake**. Так названа техника синтеза изображения на основе системы искусственного интеллекта, используемого в машинном обучении (**deep learning**). С ее помощью можно производить совмещение и наложение выбранных фото или видео на исходные фото или видео.

С чего все началось? В ноябре 2017 года в социальной сети Reddit появилась площадка **r/deepfakes subreddit** (в феврале 2018 года она была запрещена и удалена) с представленными на ней сексуально откровенными видеороликами, в которых лица субъектов были заменены лицами знаменитостей. Как впоследствии выяснилось, эти ролики размещал программист, имевший опыт работы с системами машинного обучения. Создание этих роликов было его хобби, и он развлекался, накладывая лицо какой-либо знаменитости на изображение чужой головы. В течение месяца площадка собрала более 15 тысяч подписчиков. В новом сложившемся сообществе слово **deepfake** стало использоваться и вошло в обиход для обозначения различных фальшивых видео, сгенерированных с помощью нейронных сетей.

В январе 2018 года другой пользователь сети Reddit разработал удобное в использовании мобильное приложение, с помощью которого любой, даже не имеющий

специального компьютерного образования, человек может создавать подобные видео со своим набором данных. Весь необходимый инструмент доступен бесплатно и снабжен подробными инструкциями, позволяющими новичку освоить весь процесс. Тем самым был открыт ящик Пандоры. За прошедшее время были созданы всевозможные мемы: лицо Николаса Кейджа с телом Эми Адамс и постановка с участием комика Джордана Пила в качестве бывшего президента США Барака Обамы, который предупреждает о некоторых возможных зловещих применениях цифровых технологий [5], и многие другие.

Нельзя сказать, что аналогичные компьютерные технологии не были известны и не применялись в киноиндустрии ранее. Например, в фильме «Форест Гамп» есть эпизод, в котором герой общается с президентом США Джоном Кеннеди. Однако сейчас подобный инструмент с серьезными возможностями стал доступен практически каждому.

По мнению специалистов, в настоящее время мы вплотную подошли к границе нового мира, в котором очень просто изготовить правдоподобные видеоролики о людях, делающих то, чего они никогда не делали. И это несет миру серьезную угрозу. Хотя многие подписчики **r/deepfakes subreddit** занялись изготовлением с разными целями порнографического видео (это и порнография местности, и различной природы хейтерство, и другие причины), некоторые пользователи стали создавать видеоролики иного рода. Так, например, один пользователь разместил отснятые документальные кадры с Гитлером, совмещенные с видео президента Аргентины Маурисио Макри. На YouTube можно увидеть фальшивые видео с Дональдом Трампом, Владимиром Путиным, Хилари Клинтон.

Разнообразные примеры демонстрируют возможные далеко идущие последствия использования рассматриваемой технологии, позволяющей любому, имеющему достаточный материал, разместить в сети любое лицо в любом видео и сделать это довольно убедительно. По мнению специалистов, любой, кто может загрузить и запустить **FakeApp** (мобильное приложение), может создавать подобные видео, имея лишь один-два высококачественных видеоролика или несколько фотографий лиц, которые он хочет подделать. Утверждается, что **FakeApp** — это настольное приложение, разработанное сообществом для запуска алгоритма **deepfake** без установки Python, Tensorflow и т. д. И все, что нужно иметь, — это хороший графический процессор, которого требуют высококачественные 3D-видеоигры, и поддержку CUDA (параллельной вычислительной платформы и модели программирования, разработанной корпорацией NVIDIA). Если у пользователей нет соответствующего графического процессора, его можно арендовать с помощью таких сервисов, как Google Cloud Platform. Запуск всего процесса, от извлечения данных до кадрового преобразования одного образа в другой, занимает от восьми до 12 часов.

Размывая границы между фактом и вымыслом, **deepfake**-технологии могут подорвать доверие общества к записанным изображениям и видео как объективным отражениям реальности. В настоящее время еще можно невооруженным глазом идентифицировать значительную часть подделок. Но, как и всё в цифровом мире, улучшения происходят экспоненциально. И там, где технология не сможет быть убедительной, двойственность подтверждения скомпенсирует этот недостаток.

Распространение дезинформации через социальные сети является одним из серьезнейших глобальных

рисков для нашего будущего. Опровержение дезинформации представляет очень серьезную проблему, а борьба с фальшивыми новостями оказалась совсем не простой [2]. К тому же, если содержание будет соответствовать нашим убеждениям, нас, скорее всего, не насторожит неестественное выражение лица на видео или приглушенный голос.

Политики должны проявить инициативу, а правительства разработать комплекс мер для противостояния новым угрозам. Соответствующие меры могут включать упреждающее сообщение о наказаниях — как производителям, так и издателям вредоносного контента, а также четкие протоколы для обеспечения их соблюдения.

Однако не менее важной мерой противодействия угрозам был бы охват традиционных и цифровых медиaplatform, чтобы кардинально переосмыслить систему безопасности вокруг онлайн-контента. Возникает вопрос об организации законодательной защиты граждан от действий указанного рода. Ведь только в 2015–2016 годах пользователи выгрузили на Google Photo 24 миллиарда (!) селфи. Несложно представить, что можно создать с помощью любительской программы, используя фотографии человека, которого хотят скомпрометировать. Крупные корпорации сейчас вкладывают огромные средства в разработку программ, позволяющих отличить реальное видео от подделки. А пока что специалисты по безопасности напоминают об известной возможности защитить свои фотографии во Всемирной паутине — использовать водяные знаки, а еще лучше — не размещать фотографии вовсе [1].

Вторая секция, которую посетила автор статьи, была посвящена **персональным данным**. Первоначально от участников, зарегистрировавшихся на эту секцию, попросили письменное согласие на исследование информации, которую можно найти о них в интернете, используя только легальные средства поиска. Впоследствии предполагалось, что найденная информация будет обнародована на секционном заседании. В случае обнаружения «деликатной» информации у участника будет испрошено дополнительное согласие на обнародование найденного. В действительности обещанного публичного обнародования сделано не было. Заинтересованным участникам было предложено по окончании секции подойти к ведущему и ознакомиться с результатом его поисков. Относительно автора ничего найдено не было, возможно, отчасти потому, что основной материал автора представлен на русском языке. У нескольких участников, как было видно, список найденного выглядел внушительным, но ничего обнародовано не было.

На этой секции было рассказано об инструментах, которыми пользуются профессиональные поисковики. Поиск может быть многоступенчатым. Было рассказано, какие сайты являются основными держателями персональных данных. Так, например, Amazon имеет огромный банк данных по своим покупателям, Google держит все данные по сайтам знакомств.

Данными торгуют, как товаром. Занимаются торговлей так называемые *datadating brokers* (брокеры данных).

На заседании секции приводились примеры рекламных объявлений о продаже данных и цен на эти данные. Например, объявление о предвешенной распродаже гласило: «87 мужчин и 80 женщин, курящие, выпивают в компании, по случаю, протестанты», и данные о них продавались за 95,19 долларов. А далее фрагмент данных: семейное положение, род занятий, религиозная принадлежность, рост, телосложение, цвет глаз, цвет волос и т. д. Для человека, далекого от сайтов знакомств, приведенные примеры выглядели интересными, с одной стороны, и пугающими, с другой.

Регистрируясь на каком-либо сайте, например, бронируя гостиницу или совершая покупку, человек не представляет, что его данные пополняют базу владельца сайта, и не может со стопроцентной уверенностью сказать, что его право на неприкосновенность персональных данных не будет нарушено. К тому же в сети действует онлайн-оффлайновая дихотомия, когда пользователь сети подсознательно предполагает, что с его данными онлайн-продавцы обращаются так же, как в обычном магазине, а это не так [3].

По тому, какой объем данных и за какие деньги предлагался, можно примерно представить, насколько это серьезный вид бизнеса. Представленные на секциях презентации наглядно продемонстрировали, что то, о чем пишут специалисты по безопасности, реально и очень серьезно.

Форум SIF ежегодно знакомит с новыми тенденциями, представляет новые риски и предлагает возможные пути противостояния этим рискам. В 2014 году автору довелось выступить на форуме и рассказать о совместной работе с Институтом открытого образования Архангельской области по обучению детей интернет-безопасности. Фактически SIF — это площадка для обмена мнениями, опытом, для установления новых контактов, это источник новых идей и профессионального совершенствования. Хотелось бы, чтобы наша педагогическая общность тоже была в курсе современных реалий в ситуации с детской безопасностью во Всемирной паутине.

Список использованных источников

1. Богданова Д. А. О создании и мониторинге цифровой идентичности // Современные информационные технологии в образовании: Материалы XXVIII Международной конференции (Троицк — Москва, 27 июня 2017 года). М.: Московский издательско-полиграфический колледж им. И. Федорова, 2017. С. 120–122.
2. Богданова Д. А. Об одном глобальном риске и способах борьбы с ним // Народное образование. 2018. № 3–4. С. 191–196.
3. Богданова Д. А., Бровка Н. В. Дружественный Интернет: каким его видят британские школьники // Информатика и образование. 2017. № 10. С. 54–59.
4. Safer Internet Forum. The impact of technology on children, young people and society // Better Internet for Kids. 2018. November 20. <https://www.betterinternetforkids.eu/web/portal/policy/safer-internet-forum>
5. You Won't Believe What Obama Says In This Video! // YouTube. 2018. April 17. <https://www.youtube.com/watch?v=cQ54GDm1eL0>