АЛЬЯНС
ПО ЗАЩИТЕ ДЕТЕЙ
В ЦИФРОВОЙ СРЕДЕ

Ростелеком

MINDSMITH

TEQVISER

Исследование «Технологии защиты детей в интернете»

2022

Содержание

Введение

Кибербезопасность — один из ключевых приоритетов современного цифрового общества. Дети и подростки активно пользуются интернетом, при этом они относятся к наиболее уязвимой категории пользователей: их когнитивные способности, мировоззрение и навыки критического мышления находятся в процессе формирования. В связи с этим необходимо изучать риски, с которыми несовершеннолетние могут столкнуться в интернете, а также технологические методы защиты детей и обеспечения их безопасности в онлайн-среде.

Разработка технологических методов защиты детей, направленных на обеспечение их безопасности в онлайн-среде, неразрывно связана с изучением киберрисов, представляющих угрозу для несовершеннолетних.

Исследование «Технологии защиты детей в интернете» проводилось с октября 2021 года по март 2022 года. В рамках исследования был проведен анализ киберрисков для детей и подростков, изучены технологические меры по противодействию киберрискам, определены риски, с которыми несовершеннолетние могут столкнуться в будущем, а также предложены рекомендации для стейкхолдеров.

— В основе исследования использовался искусственный интеллект (машинное обучение). Представленная информация и выводы получены с применением интеллектуальной аналитической системы выявления новых рынков, перспективных технологий и методов их использования TeqViser. Кластерный анализ проводился на основе выборки, включающей более 21 тысяч научных работ.

— На основе анализа более 500 источников литературы было выявлено 23 риска, угрожающих безопасности детей и подростков в интернете. Для определения степени опасности рисков и эффективности технологических решений по противодействию им была дана экспертная оценка от приглашенных к исследованию специалистов в области кибербезопасности, детской психологии и социологии.

— В рамках изучения технологических мер по противодействию киберрискам для детей и подростков было проанализировано более 300 патентов, компаний и ИТ-решений в области кибербезопасности детей и подростков. По результатам анализа было сформировано 8 кластеров технологических решений.

— На основании существующих рисков и ряда трендов, продиктованных технологическими, социальными и геополитическими изменениями, были определены 10 областей, в которых будут формироваться риски для несовершеннолетних в ближайшем будущем.

— По результатам исследования были предложены рекомендации для стейкхолдеров, направленные на усиление безопасности детей и подростков в интернете.

Ключевые выводы

1. Самые опасные риски связаны с психологическим насилием над ребенком

Риски, представляющие собой результат агрессивного столкновения между людьми, имеют высокую степень опасности. При этом технологические решения достаточно развиты, чтобы противостоять примитивным личностным атакам и снижать их объем, но не способны предотвратить атаки со стороны большого количества злоумышленников или тех, кто хорошо осведомлен о принципах работы технологии.

2. Решения, связанные с фильтрацией контента и защитой детей от онлайн-мошенничества, проработаны лучше других

Наиболее эффективно работают методы защиты от рисков, связанные с фильтрацией и блокировкой контента порнографического и насильственного характера, а также с предотвращением случаев онлайн-мошенничества и распространения опасных товаров. Технологические решения, направленные на противодействие этим рискам, встроены в функционал сразу нескольких кластеров технологических мер борьбы (системы родительского контроля, интернет-фильтры), а также присутствуют непосредственно на платформах, предоставляющих цифровой контент.

3. Недооценены риски, связанные с информационным и маркетинговым давлением

Риски, связанные с информационным и маркетинговым давлением, вовлечением детей в рискованные денежные отношения, а также распространением дезинформации и контента, не предназначенного для детей и подростков, в значительной степени недооценены. Хотя стейкхолдеры знают о рисках, необходимо повышение цифровой грамотности в области их профилактики, а также консолидации усилий со стороны всех вовлеченных сторон.

4. Риски будущего требуют особого внимания

В среднесрочной перспективе ожидается усиление рисков, связанных с развитием виртуальной реальности и метавселенных (рост влияния цифровых инфлюенсеров, новые возможности взаимодействия между взрослыми и детьми); искусственного интеллекта как инструмента преступной деятельности и технологии воспитания; ростом цифрового разрыва, информационных войн и цифровой изоляции; новыми угрозами приватности и персональным данным (цифровой след, биометрия).

5. Борьба с киберугрозами требует взаимодействия множества стейкхолдеров

Развитие технологий как порождающих киберриски, так и направленных на борьбу с ними, происходит крайне динамично. В процесс поиска решений в этой сфере должно быть вовлечено множество субъектов. При этом стейкхолдеры должны быть свободны в проявлении инициативы и экспериментировании. Процесс будет по-настоящему эффективным, если будет сформировано пространство совместной ответственности за результат.

Киберриски для детей и подростков

Криминализация, втягивание в криминальные практики

1. Вовлечение детей в криминальные сообщества
2. Продажа запрещенных товаров и услуг
3. Радикализация и экстремизм
4. Траффикинг

Маркетинговое давление, рискованные денежные отношения

5. Интернет как канал сбыта товаров, опасных для жизни и здоровья детей
6. Продвинутые методики маркетинга
7. Темные паттерны
8. Онлайн-мошенничество

Личностная атака, направленные против ребенка деструктивные действия

9. Кибербуллинг
10. Сталкинг
11. Груминг
12. Сексуальные домогательства

Цифровая эксплуатация, использование ребенка для создания цифрового контента

13. Доксинг
14. Создание и распространение материалов с детской порнографией
15. Кража, сбор и эксплуатация персональных данных
16. Шерентинг

Информационное давление, информация, не предназначенная для детей и подростков

17. Контент, содержащий сцены насилия
18. Порнографический контент
19. Дезинформация
20. Опасные тренды и челленджи

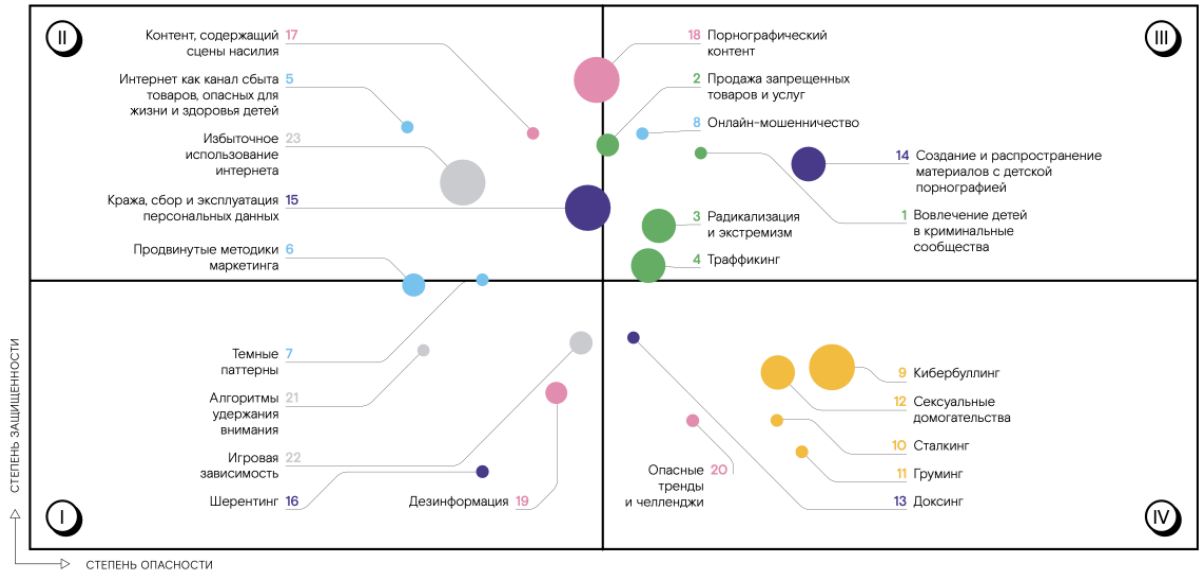
Аддикция, формирование зависимости от интернет-среды

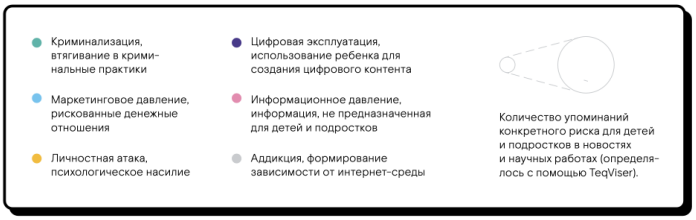
21. Алгоритмы удержания внимания
22. Игровая зависимость
23. Избыточное использование интернета

Карта киберрисков

В рамках исследования был проведен экспертный опрос, в ходе которого эксперты оценили степень опасности и степень эффективности технологических мер защиты (степень защищенности) каждого риска.

По результатам опроса мы расположили все киберриски по двум осям: «степень опасности» (ось X), «степень защищенности» (ось Y).





Таким образом, мы выделили 4 группы рисков:

1) Недооцененные — риски с низкими степенями опасности и защищенности;

2) Контролируемые — риски с низкой степенью опасностью и высокой степенью защищенности;

3) Актуальные — риски с высокими степенями опасности и защищенности;

4) Требующие внимания — риски с высокой степенью опасности и низкой степенью защищенности.

Группа 1. Криминализация, втягивание в криминальные практики

К этой группе относятся риски, которые подразумевают вовлечение детей в криминальные, запрещенные законодательством практики, например: вовлечение детей в криминальные сообщества, продажу запрещенных товаров и услуг, радикализацию и экстремизм, а также траффикинг.

Последствия таких рисков могут крайне негативно сказаться на психоэмоциональном и физическом состоянии ребенка, а также представляют опасность для общества в целом.

1. Вовлечение детей в криминальные сообщества

Детям, состоящим в группах и сообществах, пропагандирующих деструктивные действия, активно навязываются безнравственные ценности и установки. Например, обесценивание человеческой жизни, проявление агрессии и жестокости.

При этом подобные сообщества вовлекают несовершеннолетних в наркоманию, тематику социопатии, массовых и ритуальных убийств, сатанизма, анархии, нацизма, экстремизма.

Не единичны случаи вербовки людей в террористические организации через интернет, что приводит к распространению террористической идеологии на территориях отдельных стран, а также угрожает безопасности и жизнедеятельности общества в целом.

Специфика риска

Большинство специалистов признают: одна из причин роста количества предварительно расследованных особо тяжких преступлений, совершенных несовершеннолетними или с их участием за последние годы — влияние запрещенной в России криминальной субкультуры АУЕ (Арестантско-уркаганское единство, арестантский уклад един и т. д.). В числе основных целей организации — вовлечение молодежи в свои ряды и формирование смены за счет подростков.

Дети, увлекаясь подобными субкультурами, не осознают всех угроз, которые они в себе несут, причем взрослые не готовы воспринимать масштабы и характер таких угроз. Объединения АУЕ активно ведут пропаганду как через интернет, так и посредством прямой вербовки — многих вынуждают вступать туда под угрозой физического насилия.

Интернет стал площадкой формирования радикально настроенной молодежи через социальные сети, где им прививают экстремистские взгляды.

Известно, что подростки подвержены формированию установок на агрессивное поведение, поэтому дополнительную опасность для них несут:

1. возможность целенаправленной пропаганды экстремального поведения в интернете;
2. разжигание агрессии посредством экстремистских лозунгов;
3. политизация социально-экономических проблем;

4. романтизация образов «отрицательных героев» (Эрик Харрис, Дилан Клиболд,[1] Филипп Лис,[2] лидеры экстремистских и террористических организаций и др.);
5. навязывание подросткам идей, пропагандирующих насилие в качестве социальной нормы путем погружения их в деструктивные интернет-сообщества.

Подросток, особенно социально неблагополучный, всегда тянется к силе, а объединение в группы намного ее увеличивает. Нравственные установки и психологическая атмосфера ближайшего социального окружения несовершеннолетних имеют решающее значение в формировании асоциальных привычек и стереотипов поведения.

В рамках исследования один из участников преступной группировки рассказал о физическом насилии, которое применялось старшими участниками группировки для воспитания подростков. Также дети подчеркнули, насколько было сложно выйти из организованной преступной группы — девиз ОПГ: «невозможно покинуть или изменить».

Еще одной угрозой для несовершеннолетних в интернете является привлечение их к совершению преступлений, связанных с незаконным оборотом наркотиков. Вербовка проводится через популярные социальные сети «ВКонтакте», «Одноклассники», а также в даркнете.[3] Детям поступает предложение о подработке в качестве курьера, однако о том, что конкретно следует распространять, говорят не сразу. После получения согласия подростка инструктируют, где он должен получить сверток с наркотиками, где его спрятать и как отчитаться о месте закладки через приложение в мобильном телефоне.

Распространенность

В 2020 году в интернете насчитывалось около 50 тысяч ресурсов, пропагандирующих криминальную субкультуру АУЕ с охватом аудитории до 1 млн человек. В 80 % случаев подавляющее число подписчиков — дети и молодежь до 30 лет.

Среди всех преступников несовершеннолетние в целом по стране составляют примерно 4-6 %. Однако в некоторых регионах эта цифра достигает 8 % и более (Забайкальский край, Амурская область, Хабаровский край, республика Карелия), что в 2,5 раза больше удельного веса самих несовершеннолетних в структуре населения страны.

Ежегодно около 20 тысяч несовершеннолетних привлекаются к уголовной ответственности за участие в преступных группах, регистрируется свыше 100 случаев совершения преступлений несовершеннолетними в составе организованных преступных формирований.

Подавляющее число несовершеннолетних (почти 89 %) совершали преступления по мотивам, связанным с их принадлежностью к конкретной группе. В ряде случаев преступления совершались по мотивам, связанным с необходимостью обеспечить «нормальные» условия жизнедеятельности группы (обеспечивали участников группы продуктами питания, спиртными напитками, нередко — предметами одежды и т. п.); хулиганские действия — по мотивам «защиты своей территории», мести враждебной группе и т. п.

По данным Генпрокуратуры, у движения АУЕ в России больше 34 тысяч активных приверженцев в 40 регионах, из которых до 40 % — подростки в возрасте 13-17 лет.

---

[1] Эрик Харис и Дилан Клиболд — участники террористического акта, который был совершен 20 апреля 1999 года в школе "Колумбайн" (округ Джефферсон, штат Колорадо, США).
[2] Филипп Лис — администратор "группы смерти", который был признан виновным в доведении до самоубийства нескольких подростков в 2016 году.
[3] Даркнет (DarkNet) — это «надстройка» над обычным интернетом, организованная с помощью частных сетей, в которых информация шифруется несколькими способами и используются специальные правила маршрутизации.

Около 80 % участников массовых беспорядков на почве экстремизма составляет молодежь, треть из них — несовершеннолетние. Наметилась тенденция «омоложения» и повышения криминальной активности лиц в возрасте 13-14 лет, причисляющих себя к неформальным молодежным объединениям.

Примеры

Кардеры и «Доминос» (2014)

В 2014 году сеть пиццерий «Доминос» была переполнена звонками от пострадавших людей: с их карт сняли деньги за покупку пиццы в Бруклине (район Нью-Йорка). Некоторые из жертв жили на другом конце страны. С большинства карт сняли оплату за несколько заказов, некоторые из которых стоили по 50 долларов.

Злоумышленникам удалось это сделать, используя утекшие в сеть данные о банковских картах, с помощью которых люди расплачивались за заказы пиццы в приложении «Доминос». Приложение позволяло заказать пиццу, используя только данные о номере карты и адресе доставки. В одном случае злоумышленники произвели 2000 попыток заказать пиццу, пользуясь чужими деньгами.

Сопоставив адреса, заказы и другие данные, полиция арестовала 14 человек в течение 2 дней и начала допросы. Средний возраст арестованных составлял 18 лет. Оказалось, что подростки, на чей адрес была оформлена доставка, находили в соцсетях сообщения с предложением заказать пиццу «Доминос» бесплатно.

ОПГ «Белята» (2019-2021)

Участников молодежной группировки «Белята», занимавшихся мелким воровством и вымогательством, относят к последователям неформального молодежного движения АУЕ. Неформальная группировка насчитывала, по разным данным, от 20 до 70 несовершеннолетних. Они открыто рассказывали о своей деятельности в соцсетях — на странице в «ВКонтакте» с общим числом подписчиков более 1700 пользователей выкладывались «вайны»[4], на которых запечатлено избиение подростков. При этом старшие члены банды нацеливали несовершеннолетних подростков на постоянное расширение числа участников группировки. Принимали в нее добровольно, но за выход человек должен был заплатить.

11 августа 2021 года Набережночелнинский городской суд Республики Татарстан вынес приговор шестерым активным участникам группы, четверо из которых еще не достигли и 18 лет. В уголовном деле было 10 эпизодов — по всем из них фигуранты признаны виновными.

Кибератака на PayPal (2010-2011)

В 2010 году была совершена кибератака на сервис онлайн-платежей PayPal, который используется для безопасных денежных переводов при покупках в интернете. Полиция провела десятки рейдов в Великобритании, Нидерландах и США в поисках подозреваемых в организации атак со стороны хакерских групп Anonymous и LulzSec. Считалось, что атака была мотивирована решением компании PayPal прекратить обработку пожертвований в пользу WikiLeaks и ее основателя Джулиану Ассанжу.

[4] Вайны — короткие видеоролики.

В результате в августе 2011 года были арестованы 18 человек (в США — 14 человек, в Нидерландах — 4 человека). Среди них оказался 16-летний британский школьник, который взял на себя ответственность за это и другие преступления — атаки на корпоративные и правительственные веб-сайты по всему миру.

Источники

1. Борисов Евгений. «Распространение криминальной субкультуры АУЕ среди молодежи: ключевые факторы, угрозы, меры противодействия» (2020)
2. Бураева Людмила и Залина Дадова. «О проблемах негативного влияния глобального информационного пространства на процесс становления системы ценностей молодежи». Социально-политические науки № 5 (2018)
3. Голубых Никита и Константин Потанин. «Предупреждение вовлечения несовершеннолетних в деятельность деструктивных интернет-сообществ экстремистской направленности» (2020)
4. Гусева Анастасия и Станислав Шемелов. «"Белят" отправили работать: суд вынес первый приговор АУЕ — подросткам из Челнов». Бизнес-online (2021), https://www.business-gazeta.ru/article/518761
5. Ивасюк О.Н. и И.В. Калашников. «Криминологические особенности современной преступности несовершеннолетних» (2019)
6. Костенко Ярослава и Елена Сидоренко. «АУЕкнулось: почему приверженцев воровской идеологии признали экстремистами». Известия (2020), https://iz.ru/1048836/iaroslava-kostenko-elena-sidorenko/aueknulos-pochemu-priverzhentcev-vorovskoi-ideologii-priznali-ekstremistami
7. Кузнецов Артем и Анастасия Гусева. «"Белята", "Маслята" и "48-й комплекс": как в Челнах зачищают АУЕ». Бизнес-online (2019), https://www.business-gazeta.ru/article/445025
8. Куликов Алексей. «О некоторых аспектах оперативно-розыскного противодействия колумбайну в социальных сетях». Проблемы правоохранительной деятельности № 4 (2021)
9. Мазуров Валерий и Стародубцева Мария. «Экстремизм и терроризм в киберпространстве: угрозы миру и безопасности человечества». Сборник статей по итогам III Всероссийской студенческой научно-практической очно-заочной видеоконференции (2020)
10. Прозументов Лев. «Криминологическая характеристика преступности несовершеннолетних» (2004)
11. Смыслова Вера. «Вовлечение молодежи в социальную практику и активную общественную деятельность как одно из направлений противодействия проявлениям молодежного экстремизма в условиях радикализации и роста протестной активности» (2017)
12. Тарасов Алексей. «Страна из трех букв». Новая газета (2020), https://novayagazeta.ru/articles/2017/06/16/72816-strana-iz-treh-bukv
13. Тимошина Елена. «Деструктивные субкультуры несовершеннолетних как условия их виктимизации и криминализации» (2021)
14. Хатуев В. Б. «История становления и развития российского уголовного законодательства об ответственности за склонение к самоубийству и содействие ему». Вестник Московского университета. Серия 11. Право 4 (2018)
15. Ashton, Sally-Ann and Anna Bussu. «Peer groups, street gangs and organised crime in the narratives of adolescent male offenders» (2020)
16. Camber, Rebecca. «Global crackdown on hackers: British teen arrested along with 14 suspected members of «Anonymous» group». Daily Mail (2010), https://www.dailymail.co.uk/news/article-2016451/Anonymous-hackers-arrested-15-suspected-members-total-including-British-teen.html
17. Wilson, Michael. «Pizza Orders Reveal Credit Card Scheme, and a Secondhand Market». New York Times (2014),

https://www.nytimes.com/2014/12/06/nyregion/pizza-orders-reveal-credit-card-scheme-and-a-secondhand-market.html

2. Продажа запрещенных товаров и услуг

Интернет дает возможность приобретать товары и услуги, свободная реализация которых запрещена или ограничена законодательством. Наиболее популярный запрещенный товар, который несовершеннолетние покупают через интернет — наркотики.

Кроме того, в интернете подростки могут купить нелегальное оружие, заказать услуги по взлому компьютеров, телефонов, аккаунтов в соцсетях и приложениях. Обычно для этого используют даркнет, обеспечивающий анонимность покупателя и продавца.

Детям и подросткам сложнее, чем взрослым, придерживаться правил поведения и моральных ценностей в интернете. Они могут приобретать запрещенные товары и услуги из любопытства или ради чувства причастности к определенной группе людей.

Специфика риска

Наиболее популярным нелегальным товаром, который можно приобрести в интернете, независимо от возраста покупателя, являются наркотические вещества. Возраст людей, страдающих наркотической зависимостью, снижается. Сейчас наркоманами становятся подростки уже в возрасте 13-15 лет, что связывают в том числе с легкостью покупки наркотиков.

Продажа наркотиков происходит полностью анонимно. Для этого, как и для сбыта большинства нелегальных товаров и услуг, используется даркнет, обеспечивающий более высокую степень анонимности для пользователей.

Подростки могут приобрести в интернете оружие для использования его в деструктивных и общественно опасных целях. В отличие от западного теневого рынка, в России данная практика менее распространена. Несмотря на это, на крупнейших онлайн-платформах можно найти нелегальное оружие и приобрести его.

К услугам, которые дети и подростки могут заказать в интернете, относится взлом компьютеров, телефонов, аккаунтов в социальных сетях и приложениях. Так, благодаря фишингу,[5] вредоносному программному обеспечению, а также другим технологическим и психологическим видам атак, которые используют наемные хакеры, у заказчика появляется возможность получить доступ к конфиденциальной информации о другом человеке.

Наконец, благодаря интернет-пиратству дети могут скачивать игры, приложения, программное обеспечение, не приобретая лицензионную версию, что не только нарушает авторские права, но и может угрожать безопасности устройства ребенка.

Причины

Причины, которые могут спровоцировать детей на покупку и употребление наркотических веществ, включают в себя социальные, психологические и другие факторы. При этом в отличие от взрослых, которые принимают наркотики ради расслабления или эйфории, дети и подростки часто пробуют их из любопытства или ради причастности к группе людей, которая им это предлагает.

[5] Фишинг (англ. phishing от fishing «рыбная ловля, выуживание») — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

Среди причин, по которым подростки покупают оружие, выделяют социальные и психологические аспектах: конфликты, низкий уровень жизни, неблагополучные районы проживания, социальная изоляция, психологические травмы. Также причинами могут послужить девиации в поведении из-за чрезмерного влияния интернета или отдельных субкультур.

Дети и подростки не всегда могут правильно оценить последствия своих действий. В частности, это может быть причиной отношения к компьютерному пиратству как к забаве или поводу для хвастовства.

Распространенность

За 2020 год сотрудниками Национального центра информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет (НЦПТИ) было выявлено 709 ссылок на противоправный контент. Из них 147 ссылок — на наркотический контент, а 138 — на материалы, причиняющие вред здоровью и развитию детей.

Ежегодно в России на наркотики тратят более триллиона рублей, при этом по разным оценкам, страдают от наркотической зависимости 5-8 млн человек. Важно отметить, что несовершеннолетние — часть наркобизнеса: они могут выступать как в роли потребителя, так и в роли продавца. По статистике, за наркопреступления в России каждый день судят 6 подростков.

Дети до 16 лет составляют примерно 20 % от общего количества наркозависимых, а средний возраст человека, начинающего принимать наркотические вещества, варьируется от 15 до 17 лет. По результатам медико-социальных исследований, средний возраст приобщения к наркотическим средствам снизился соответственно до 14,2 лет среди мальчиков и 14,6 лет среди девочек. При этом подростки злоупотребляют наркотиками в 7,5 раз чаще, чем взрослые.

Что касается нелегального оборота оружия, согласно официальной статистике МВД, в 2018-2020 годах из незаконного оборота было изъято более 67 тысяч единиц огнестрельного оружия и зарегистрировано свыше 130 тысяч преступлений в этой сфере.

Примеры

Покупка аккаунта каршеринга (2018)

По данным СМИ, семнадцатилетний юноша купил аккаунт пользователя каршеринга в интернете и получил доступ к управлению автомобилем. В результате произошла авария — автомобиль попал в занос и перевернулся. Водитель и еще двое подростков, которые были пассажирами, госпитализированы.

Продажа аккаунтов пользователей каршеринга — довольно распространенное явление. Предложения можно без труда найти на форумах, в Telegram-каналах и в даркнете.

Перепродажа наркотиков, купленных за криптовалюты (2018-2021)

Подростки используют криптовалюты для покупки в даркнете наркотиков, а затем перепродают их в школе. По утверждению полиции, речь идет не об опытных преступниках, а именно о подростках, так как новые технологии размывают возрастные барьеры для совершения преступлений.

В графстве Корнуолл, Великобритания, недавний рост употребления наркотиков связывают именно с покупкой запрещенных веществ в даркнете. Также сообщалось о смерти 15-летней Шакиры Пеллоу после употребления таблеток, содержавших МДМА. Трое других подростков были доставлены в больницу после приема того же наркотика. Вещество представляло собой маленькие голубые таблетки с маркировкой игрушек фирмы LEGO.

Источники

1. Архипова А.Д. «Предупреждение преступлений несовершеннолетних, связанных с незаконным оборотом наркотических средств». Скиф. Вопросы студенческой науки № 11 (2019)
2. Войскунский Александр и др. «Этическая направленность подростков и молодежи в социальных сетях». Психологические исследования 7.37 (2014)
3. Гадельшин Артем и Егор Потапов. «Оружейная культура в РФ. Причины скулшутинга и пути его предотвращения». Вопросы российской юстиции 13 (2021)
4. Горяинова Н.А. и Ю.В. Чепрасова. «Формирование здорового и безопасного образа жизни несовершеннолетних с учетом негативной информации сети интернет, связанной с незаконным оборотом наркотических и психоактивных веществ». Грани педагогики безопасности (2018)
5. Лаптев Леонид и Виктор Закатов. «Социально-психологические условия эффективной профилактики наркозависимости формирующейся личности подростка». Проблемы эффективной интеграции инновационного потенциала современной науки и образования (2018)
6. Ломакин А. С. и В. В. Боровик. «Исследование влияния доступа к интернету на психику детей». Человек в цифровой реальности: технологические риски: материалы V Международной научно-практической конференции, посвященной 75-летию Победы в Великой Отечественной войне (2020)
7. Петрова Дарья и др. «Проблемы профилактики наркозависимости среди несовершеннолетних». Человеческий капитал № 3 (2015)
8. Чурилов Сергей и др. «К вопросу об информационной безопасности подростков в социальных сетях и сети интернет». Формирование гражданской устойчивости как фактор противодействия идеологии экстремизма и терроризма (2017)
9. Шеллер Игорь. «Darknet — темная сторона интернета». Наука через призму времени (2018)
10. Якунин Иван. «Каршеринг оказался доступным для "водителей" без прав». Коммерсантъ (2018), https://www.kommersant.ru/doc/3516138
11. «В Девоне подросток покупал наркотики за биткоин». MyCrypter (2021), https://mycrypter.com/v-devon-podrostok-pokupal-narkotiki-za-bitkoin/
12. Spalevic, Zaklina and Milos Ilic. «The use of dark web for the purpose of illegal activity spreading». Ekonomika, Journal for Economic Theory and Practice and Social Issues (2017)
13. Wood, Jessica A. «The Darknet: A Digital Copyright Revolution». Richmond Journal of Law & Technology 16.4 (2009)

3. Радикализация и экстремизм

Подростки наиболее восприимчивы к радикальным националистическим, ксенофобским и экстремистским идеям.

Часто в экстремистские и радикальные организации вербуют через социальные сети. Кроме того, алгоритмы рекомендательных сервисов настроены на показ информации в зависимости от интересов пользователя.

Если ребенок заинтересовался радикализацией определенной формы, вероятность того, что алгоритмы порекомендуют контраргументы, способные его переубедить, крайне мала. Система может направить пользователя к сообществам радикалов, каналам пропаганды и материалам, которые только углубят его наклонности и укрепят экстремистские взгляды.

Специфика риска

Экстремистская организация определяется как общественное или религиозное объединение либо иная организация, в отношении которых, по основаниям, предусмотренным федеральным законом, судом принято вступившее в законную силу решение о ликвидации или запрете деятельности в связи с осуществлением экстремистской деятельности.

Определение экстремизма разнится в зависимости от государства или организации, а также культурного, исторического, политического, социального и других контекстов, окружающих государство или организацию. Термин «экстремизм» не имеет интернационального определения, так как данные контексты в каждом государстве свои.

Экстремистские организации используют интернет для набора новичков, индоктринации и распространения своей идеологии. По данным ООН, экстремистские сообщества не просто способны координировать свои действия и распространять произведенные материалы — они могут использовать таргетированную рекламу благодаря тому, что дети и подростки оставляют цифровой след и большой объем информации о себе в соцсетях. Сообщества радикалов используют видеозаписи, картинки, инфографики, чаты, соцсети и другие инструменты, доступ к которым им дает интернет. Более того, некоторые тактики вербовки, используемые офлайн, успешно применяются онлайн.

Тем не менее, радикализация и становление экстремистом не всегда происходит исключительно из-за деятельности экстремистской организации. По данным Совбеза ООН, попытки терактов в Европе чаще всего предпринимались преступниками-одиночками, которые ориентировались на деятельность ИГИЛ (запрещенная в России террористическая организация), но не состояли в террористических ячейках и не всегда использовали взрывные устройства. По результатам расследований, поступки этих преступников нередко были связаны с радикализацией из-за интернета — она придавала контекст неблагоприятным социальным и финансовым условиям, в которых оказывались преступники.

Веб-сайты собирают информацию о пользователях, чтобы формировать потоки рекомендованного контента. Так сайты с большей вероятностью дают своей аудитории контент, который будет интересен каждому человеку. При этом они исключают ту информацию, в которой пользователь, по их данным, не заинтересован. Рано или поздно пользователь оказывается в ограниченном потоке информации из повторяющихся мнений, тематик, форматов и создателей контента. Более того, в большинстве случаев сайты не спрашивают у

пользователей, хотят ли они формировать рекомендации на основе потребленного ранее контента. Из-за этого человек, который проявляет интерес к экстремизму определенной формы, скорее всего не увидит в рекомендациях контраргументы, способные его переубедить. Алгоритмы направят пользователя в радикальным сообществам, каналам и материалам, которые только углубят экстремистские наклонности и взгляды.

Помимо этого формируется информационная среда, в которой человек не встречает альтернативных мнений, в результате чего нормы в этой среде смещаются к все более радикальным. Чаще всего позиция формируется натурально вследствие выбора человеком своего окружения и вступления в сообщества, которые человека интересуют. В таком сообществе может вестись диалог, но доминантная точка зрения определена, и альтернативные мнения быстро заглушаются рядовыми и авторитетными членами сообщества. В итоге посыл приобретает все более и более крайнюю степень.

В своем интервью изданию Quartz Билл Гейтс сказал: «Технологии, такие как социальные сети, позволяют вам знакомиться с людьми, которые уже на вас похожи по взглядам. Так что вы не обмениваетесь разными точками зрения, не смешиваете их. Это очень важно, и это оказалось куда большей проблемой, чем я и многие другие ожидали». Люди могут состоять в нескольких сообществах, доминантные мнения в которых противоположны, и самостоятельно общаться с политическими оппонентами. Несмотря на это, люди чаще делятся информацией от источников, которые на них идеологически похожи.

Распространенность

По данным МВД России, число случаев экстремизма с января по сентябрь 2021 года увеличилось более чем на 30 % по сравнению с аналогичным периодом 2020 года — 854 эпизода. В то же время количество преступлений террористического характера снизилось на 4 % — 1776 случаев. При этом 46 терактов было предотвращено, а каждое 35-е правонарушение (2,9 %) было совершено несовершеннолетними либо с их участием.

В результате проведенного группой компаний Infowatch мониторинга содержания социальных сетей Рунета установлено, что в социальных медиа есть множество деструктивных групп, в которые входят подростки и молодежь (анархизм — более 697 тысяч пользователей, нацизм — более 48 тысяч пользователей, школьные теракты — более 18 тысяч пользователей).

В 2020 году было выявлено 473 случая противоправной экстремистской направленности, совершенных с использованием интернета. По инициативе МВД России Роскомнадзором было заблокировано свыше 100 тысяч интернет-ресурсов и материалов, содержащих экстремистские призывы, удалено более 7,5 тысяч материалов экстремистского характера.

В 2020 году сотрудниками НЦИПТИ было выявлено 424 ссылки на экстремистские и террористические материалы.

Преступления экстремистской направленности чаще всего совершают подростки 14-17 лет. Причем большинство из них — учащиеся вузов и средних специальных учебных заведений. Высокий процент подростковой экстремистской преступности связан с тем, что именно возраст от 14 до 18 лет наиболее оптимален для «впитывания» радикальных националистических, ксенофобских и экстремистских идей, следовательно, лиц данной возрастной категории проще всего идеологически подготовить для совершения экстремистских акций.

За 2018 год Судебным департаментом при Верховном суде РФ, было осуждено 555 человек по статьям, связанным с экстремизмом. 12 % (71 человек) из них были в возрасте 14-17 лет, а 33 % были в возрасте 18-24 лет. За 2020 год было осуждено 288 человек по тем же статьям. Возрастная группа 14-17 лет составила 4 % (12 человек), а возрастная группа 18-24 лет составила 20 % (59 человек) от осужденных.

Примеры

«Новое величие» (2017-2021)

В марте 2018 года сотрудники правоохранительных органов задержали десятерых участников «Нового величия», часть из них — несовершеннолетние. По версии следствия они хотели совершить государственный переворот для захвата власти в России. При этом сторона защиты утверждает, что инициатива по созданию сообщества якобы принадлежит сотрудникам полиции и спецслужб, которые подстроили эту провокацию в отношении обвиняемых.

В отношении подростков было возбуждено уголовное дело по частям 1 и 2 статьи 282.1 Уголовного кодекса («Организация экстремистского сообщества и участие в нем»). Их поместили под стражу и под домашний арест.

Вербовка несовершеннолетних (2021)

В декабре 2021 года двадцатилетний молодой человек из Нижнего Новгорода создал в мессенджере чат, с помощью которого вербовал в террористы несовершеннолетних, проживающих в Нижегородской области. Мужчина также проповедовал идеологии экстремистских организаций. Во время обыска у него дома нашли предметы, подтверждающие факт причастия к вербовке.

Школьники собирались взорвать здание ФСБ в игре (2020)

Летом 2020 года четырнадцатилетние школьники из Красноярска Никита и Денис расклеивали по городу листовки в поддержку арестованного анархиста. Одну из листовок молодые люди разместили на здании ФСБ. На следующий день Дениса и Никиту и еще пятерых подростков задержали. Первоначально их отпустили, но изъяли мобильные телефоны. После проверки переписок мальчиков было установлено, что они построили здание ФСБ в компьютерной игре и собирались его взрывать. Сразу после этого трое подростков, включая Никиту и Дениса, были задержаны.

Изначально школьникам было предъявлено обвинение по статье 205.3 УК РФ («Прохождение обучения в целях совершения террористической деятельности»). Двое из них признали свою вину. Денис и еще один подросток были отправлены под домашний арест, а Никита был помещен под стражу.

Онлайн-библиотека экстремистской литературы (2021)

18-летний Мэттью Кронджейгер из Уэссекса создал онлайн-библиотеку, в которой хранились экстремистские материалы и руководства по созданию взрывчатки. Он также пытался купить распечатанное на 3D-принтере оружие и собрал вокруг себя сообщество единомышленников. Будучи лидером крайне правой ячейки, Мэттью часто говорил со своими сообщниками по поводу фашистской революции и других неонацистских тем. Он также планировал убить своего

бывшего друга за то, что тот вступал в отношения с белыми женщинами. Мэттью был приговорен к 11 годам тюрьмы.

Источники

1. Василишина Юлия. «Втягивал подростков: 20-летнего нижегородца подозревают в вербовке террористов». Комсомольская правда (2022), https://www.nnov.kp.ru/daily/27350/4531412/
2. Воронин Михаил и Елизавета Демидова-Петрова. «Корреляция криминогенности несовершеннолетних и проявлений экстремизма в молодежной среде» (2020)
3. Дамаскин О.В. и В.В. Красинский. «Криминологическая характеристика механизма вовлечения несовершеннолетних в противоправную деятельность» (2020)
4. Мусаелян Марат. «Личность участника неформальных молодежных экстремистских организаций (группировок)», Адвокат № 7 (2010)
5. Шимаев Роман. «Во время заседания: фигуранты дела "Нового величия" порезали себе руки в суде». Russia Today (2019), https://russian.rt.com/russia/article/678017-novoe-velichie-incident-sud-advokaty
6. Шляпникова Ольга и Николай Паршин. «Влияние интернета на формирование противоправного поведения в подростково-молодежной среде» (2021)
7. «В Красноярском крае троих подростков обвиняют по статье об участии в террористическом сообществе». ОВД-Инфо (2020), https://ovd.news/express-news/2020/11/21/v-krasnoyarskom-krae-troih-podrostkov-obvinyayut-po-state-ob-uchastii-v
8. Barbera, P. et al. «Tweeting From Left to Right: Is Online Political Communication More Than an Echo Chamber?» (2015)
9. Bozdag, Engin. «Bias in algorithmic filtering and personalization» (2013)
10. Cho, Jaeho et al. «Do Search Algorithms Endanger Democracy? An Experimental Investigation of Algorithm Effects on Political Polarization» (2020)
11. Kaluža, Jernej. «Habitual Generation of Filter Bubbles: Why is Algorithmic Personalisation Problematic for the Democratic Public Sphere?» (2021)
12. Nguen, C. «Escape the echo chamber» (2018)
13. Wolfowicz, M. et al. «Examining the interactive effects of the filter bubble and the echo chamber on radicalization» (2021)
14. «Eleventh report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat» (2020)
15. «Filter bubbles are a serious problem with news, says Bill Gates». Quartz (2017)
16. «Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System». UN (2017)
17. «Neo-Nazi Matthew Cronjager jailed for plotting terrorist acts». BBC (2021), https://www.bbc.com/news/uk-england-essex-58973060
18. «Preventing Terrorism and Countering Violent Extremism and Radicalization That Lead to Terrorism: A Community-Policing». OSCE (2014)

4. Траффикинг

Жертв траффикинга или торговли людьми, большинство из которых женщины и подростки, принуждают к проституции, насильно заставляют работать, убивают для продажи органов на трансплантацию, незаконно усыновляют (удочеряют).

Помимо этого, интернет открыл новые формы работы и коммерциализации. Например, видеотрансляции в реальном времени, в которых преступник получает деньги за бесчеловечные действия по отношению к ребенку.

Преступники могут находить потенциальных жертв в онлайн-чатах, для этого они занимаются развитием сообществ, профилированием жертв, и даже используют рекламу. Интернет также дает возможность находить покупателей — рекламировать жертв траффикинга, привлекать клиентов и сообщников. При этом реальные данные преступников и история их злодеяний скрыта за барьерами закрытых сообществ и в даркнете.

Специфика риска

Траффикинг (торговля людьми) — это осуществляемые в целях эксплуатации вербовка, перевозка, передача, укрывательство или получение людей, введение в положение эксплуатации или удержание в этом положении путем применения насилия или угрозы его применения или других форм принуждения, похищения, мошенничества, обмана и злоупотребления доверием, властью или уязвимостью положения, либо подобных обещаний для получения согласия лица, контролирующего другое лицо. Торговля людьми — серьезная социальная проблема, представляющая опасность для фундаментальных прав человека: на жизнь, на свободу передвижения, на то, чтобы не подвергаться пыткам.

Траффикинг состоит из трех основных элементов: действие (вербовка, перевозка, передача и др.), средство (силой или угрозой ее применения) и цель (эксплуатация, подневольное состояние или извлечение органов).

Роль интернета в торговле людьми

По данным Европола, интернет является ключевым инструментом злоумышленников. Распространение интернета указывается как одна из четырех ключевых причин существования траффикинга. Логистика таких преступлений и слежка за жертвами сильно зависят от интернета. Торговля людьми приобретает совершенно другую форму, если в ней используются новые технологии: прибыль значительно растет, риски снижаются, само преступление упрощается, появляется доступ к мировому рынку клиентов и торговцев.

По информации ООН, преступники способны заниматься профилированием жертв, вовлекать людей в незаконную деятельность через рекламу онлайн. Благодаря даркнету преступники могут сохранять анонимность, не раскрывая свои личные данные. Они могут даже не продавать порабощенного им ребенка — интернет открыл новые формы траффикинга. Например, онлайн-трансляции, в ходе которых преступник получает деньги за совершение жестоких и унизительных действий по отношению к ребенку.

Из-за недоработок в законодательствах многих стран и отсутствия практики у правоохранителей раскрываемость такого рода преступлений сравнительно мала. Интернет стал площадкой для обеспечения коммерческой успешности сделок, связанных с сексуальной эксплуатации детей.

Он позволяет обеспечивать анонимность — скрывать свое местоположение и оплачивать услуги криптовалютами, что значительно затрудняет или делает практически невозможным отслеживание данных отправителя и получателя средств.

Интернет используют для вербовки потенциальных жертв, а интерес людей к контенту, пропагандирующему насилие, только облегчает этот процесс. Немаловажную роль в вербовке играют социальные сети — их особенностью является то, что с психологической точки зрения пользователь воспринимает свою страницу как некое личное пространство. Однако торговцы людьми изучают пользователей по активности в социальных сетях, в том числе анализируя комментарии к сценам с насилием, а также ценности, проблемы и желания потенциальных жертв.

Жертвы траффикинга

Жертвой торговли людьми может оказаться кто угодно, независимо от пола, возраста, национальности и религиозных убеждений. Однако важным фактором риска является юный возраст. Большинство жертв траффикинга, попавших в рабство, составляют женщины, а также дети и подростки. Это объясняется их пассивностью и покорностью: как правило, представители этих половозрастных категорий не оказывают сопротивления при психическом и физическом насилии и легко управляемы.

Жертвами траффикинга зачастую становятся лица, испытывающие серьезные финансовые трудности, оставшиеся без средств к существованию. Помимо этого, жертвами торговли людьми все чаще становятся несовершеннолетние: сексуализация подростков и детей в интернете приводит к повышенному спросу на услуги сексуального характера, оказываемые несовершеннолетними. При этом наблюдаются противоречия между желаниями молодежи и реальными возможностями потребления: роскошный образ жизни, транслируемый в СМИ, фильмах или соцсетях, приводит к тому, что дети хотят добиться его любой ценой. Данные предпосылки подкрепляются тем, что дети и подростки недостаточно информированы об опасностях и угрозах, связанных с работой в другой стране. Они часто мыслят оптимистично и не осознают риски, которым могут подвергнуть себя.

Последствия торговли людьми

Отрицательные последствия траффикинга для его жертв многочисленны. Среди них можно выделить проблемы, оказывающие влияние на социальный и экономический статус, юридическую защиту, психическое и физическое здоровье, жизнь и безопасность жертвы.

Несовершеннолетние жертвы траффикинга чаще всего подвергаются сексуальной эксплуатации, принудительному вступлению в брак, незаконному усыновлению с целью принудительного совершения преступлений или для изъятия органов и тканей. Помимо этого, среди последствий выделяют эксплуатацию в нищенстве и вербовку детей в экстремистские и террористические группировки.

Распространенность

В США примерно 40 % жертв торговли людьми в целях сексуальной эксплуатации вербуются онлайн, что делает интернет наиболее распространенным местом, где происходит вербовка жертв. Если в 2009 году количество исковых заявлений по делу траффикинга с использованием интернета насчитывало в среднем 5 заявлений при 23 потерпевших, то на момент 2018 года

глобальная сеть стала инструментом злоумышленников в 27 случаях и затронула 160 потерпевших.

С 2016 по 2020 год численность жертв детского труда впервые в истории статистического мониторинга не сокращалась, а росла: на 8,4 млн жертв за четыре года, причем почти 80 % (6,5 млн жертв) из этих детей оказались вовлечены в наиболее опасные формы труда. Официальная статистика ООН свидетельствует, что дети сейчас составляют 30 % всех жертв траффикинга: 23 % девочек и 7 % мальчиков.

США и Западная Европа — регионы с наименьшей долей детей среди пострадавших. Россия имеет худший показатель, число несовершеннолетних жертв траффикинга здесь составляет 30-50 %.

Среди организованной преступности торговля людьми занимает третье место по прибыльности, уступая только торговле наркотиками и оружием по всему миру. По оценкам, ежегодный доход от торговли людьми составляет 150 млрд долларов — это крупнейший в мире источник незаконной торговли.

Ежегодно принуждаются к браку более 12 млн несовершеннолетних девочек и девушек — лидерами по данному виду правонарушений являются страны Ближнего Востока, большинство стран Африки, а также некоторые государства Азии и Латинской Америки.

В 2019 году Национальная горячая линия США по борьбе с торговлей людьми выявила 22 326 переживших рабство, среди которых 14 597 подверглись секс-траффикингу, а 1048 — сексуализированной и трудовой эксплуатации или принуждению к работе путем обмана и шантажа. Самые распространенные направления торговли людьми — сельское хозяйство и домашняя прислуга. Большинству пострадавших в среднем 17 лет.

На начало 2020 года насчитывалось 160 млн детей, ставших жертвами эксплуатации — это каждый десятый ребенок в мире. Из них 79 млн жертв были вовлечены в самые опасные формы детского труда: выполняли работу, напрямую угрожающую здоровью, безопасности или нравственному развитию. Более половины всех жертв приходится на возрастную группу 15-17 лет.

Примеры

Вербовка для сексуальной эксплуатации (2021)

Преступник пытался через интернет завербовать несовершеннолетнюю девочку для сексуальной эксплуатации. Вербовщик высылал жертве фотографии интимного характера и провел довольно кропотливую работу по психологическому прессингу.

Узнав об этом, родители девочки подали заявление в полицию. Полицейские сразу начали проводить следственные действия под прикрытием — офицер полиции выдавала себя за пострадавшую, проводила разговоры, назначала встречи, и после долгих дискуссий было выявлено, что, помимо этой жертвы, были и другие. С преступником удалось назначить встречу и провести задержание.

Backpage (2010-2018)

Backpage — ранее действовавший американский сайт, который рекламировал услуги и товары, включая услуги сексуального характера. Именно от рекламы этих услуг сайт получал до 80 % прибыли. В 2017 году оказалось, что за частью таких услуг стояли преступники, продававшие педофилам детей. Одним из этих педофилов был Джеффри Фаррел Дэвис, 36-летний учитель средней школы. Он использовал сайт, чтобы купить у злоумышленников доступ к 14-летней жертве.

Позже Джеффри был пойман и приговорен к 10 годам в федеральной тюрьме и оштрафован на 5000 долларов. Он также был приговорен к выплате в размере 3000 долларов в качестве реституции жертве.

Источники

1. Арзуманов Илья. «Детское рабство: каждый 10-й ребенок в мире подвергается эксплуатации». Плюс один (2021), https://plus-one.ru/society/2021/07/23/detskoe-rabstvo
2. Бухоризода Б. Р. «Социальные сети и Интернет: новая форма совершения торговли людьми». Академическая мысль 2 (7) (2019)
3. Гришина Нина. «Работорговля в Африке как часть международного криминала». Азия и Африка сегодня № 12 (2018)
4. Петросян Сильва и Гегине Хачатрян. «Торговля людьми (траффикинг)» (2013)
5. Прокопенко Ольга и др. «Противодействие торговле людьми: правовые и экономические аспекты». Право и практика (2017)
6. Силуянова Юлия. «Борьба с торговлей детьми в России: поиски решения проблемы». Государственное управление. Электронный вестник № 81 (2020)
7. Силуянова Юлия. «Факторы, производство, развитие, промышленность, торговля, люди в России и в мире» (2019)
8. «Доклад ООН: пандемия усугубила угрозу торговли людьми, особенно для женщин и девочек». Русская служба новостей ООН (2020)
9. «Обещание лучшей жизни. Как дети попадают в секс-рабство». Утопия (2020), https://clck.ru/ehZiH
10. «Серджиу Руссу: "Жертвы торговли людьми не всегда понимают, что они жертвы"». Forbes.kz (2021), https://forbes.kz/process/serdjiu_russu_jertvyi_torgovli_lyudmi_ne_vsegda_ponimayut_chto_oni_mogut_rasschityivat_na_pomosch/
11. Malo, Sebastien. «Film exposes underworld of U.S. children sold online for sex». Reuters (2017), https://www.reuters.com/article/usa-trafficking-film-idINL1N1FS0L8
12. Whitcomb, Dan. «Florida man imprisoned for trafficking girl, 14, via Backpage.com». Reuters (2019), https://www.reuters.com/article/us-florida-humantrafficking-idUSKCN1S62IK
13. «Chapter v traffickers use of the Internet». UNODC (2020)
14. «Gainesville Man Sentenced to 120 Months in Prison for Obtaining Minor for Commercial Sex». Department of Justice U.S. Attorney’s Office, Northern District of Florida (2019)
15. «Global Report on Trafficking in Persons». UNODC (2018)
16. «Good Use and Abuse: The Role of Technology in Human Trafficking». United Nations Office on Drugs and Crime (2021)
17. «Situation Report Trafficking in human beings in the EU». Europol (2014)
18. «Traffickers abusing online technology, UN crime prevention agency warns». United Nations (2021)

Группа 2. Маркетинговое давление, рискованные денежные отношения

К этой группе относятся риски, в основе которых лежат маркетинговые инструменты, паттерны поведения и тонкие психологические уловки, созданные для манипуляции детьми, например: сбыт товаров, опасных для жизни и здоровья детей, продвинутые методики маркетинга, темные паттерны и онлайн-мошенничество.

Маркетинговые, психологические и дизайнерские инструменты, использующиеся как законно, так и незаконно, чаще всего нацелены на извлечение финансовой выгоды, однако в некоторых случаях могут привести и к другим серьезным последствиям.

5. Интернет как канал сбыта товаров, опасных для жизни и здоровья детей

Дети формируют собственный рынок сбыта и убеждают родителей приобретать определенные товары. В то же время они не способны проанализировать качество потенциальной покупки, а родители не всегда тщательно проверяют покупки.

Реклама и продажа детям некачественных, опасных товаров может привести к целому спектру негативных последствий — в первую очередь, они касаются здоровья ребенка.

В некоторых случаях детские товары содержат токсичные вещества в концентрации, в несколько раз превышающей допустимую. Они раздражают кожу и слизистую оболочку, отрицательно воздействуют на репродуктивную функцию человека, могут вызвать аллергию и даже рак.

Специфика риска

К вредным веществам относят природные или искусственные токсичные химические соединения, включающие в себя свинец, ртуть, полихлорированные дифенилы (ПХД), растворители и пестициды. Дети очень уязвимы к токсинам окружающей среды, поэтому предусмотрены обязательные требования безопасности к продукции, предназначенной для детей и подростков по показателям химической, биологической, механической и термической безопасности в целях защиты жизни и здоровья подрастающего поколения.

Основными сегментами детских товаров являются продукты питания, игрушки, одежда и обувь, косметика, электроника и канцелярские товары. К самым распространенным опасным товарам может относиться продукция следующих категорий: автомобильные кресла, игрушки, умные устройства, школьные принадлежности, коляски и прочие товары для детей.

В результате проведенных исследований было выявлено, что почти в каждом пятом предназначенном для детей товаре есть токсичные вещества в концентрации, превышающей допустимую в несколько раз. В таком количестве эти субстанции представляют опасность даже для взрослых: они раздражают кожу и слизистую оболочку, отрицательно воздействуют на репродуктивную функцию человека, могут вызвать аллергию и даже спровоцировать развитие онкологических заболеваний. Среди них — бор, нафталин, формальдегид. Эксперты обнаружили их в колясках, беговелах, цветных карандашах, слаймах и других игрушках.

Потребительские риски возникают в процессе приобретения товаров и услуг через интернет. Они включают риск приобретения товара низкого качества, контрафактной и фальсифицированной продукции, риск потери денежных средств без приобретения товара или услуги, хищения финансовой информации с целью мошенничества.

Реклама может оказывать как положительное, так и негативное влияние на поведение детей. Возраст ребенка играет ключевую роль в воздействии рекламных роликов на сознание и подсознание. Маленькие дети не понимают концепции коммерческого предложения. Они склонны верить тому, что им говорят, и даже могут считать себя обделенными, если у них нет рекламируемой продукции. В среднем ребенок видит более 20 000 рекламных роликов в год. Более 60 % рекламных роликов демонстрируют засахаренные хлопья, конфеты, жирную пищу и игрушки. По данным ряда исследований, дети в возрасте до 8 лет в силу своего развития не способны понять разницу между рекламой и другим контентом.

Большое влияние на молодое поколение пользователей оказывают блогеры и инфлюенсеры. По данным опроса, наряду с киноактерами и музыкантами, молодое поколение пользователей предпочитает подписываться в социальных сетях на геймеров, звезд киберспорта и видеоблогеров. В среднем 30 % молодых пользователей доверяют мнению и рекомендациям любимых блогеров, в том числе при выборе товаров. При этом дети часто сами не являются покупателями, но их мнение влияет на тот выбор, который делают их родители при совершении финальной покупки.

Распространенность

С 2020 по 2021 год увеличилось количество игрушек, не соответствующих стандартам безопасности, которые продаются через сторонних продавцов в Великобритании и в США.

Специалисты британской некоммерческой потребительской организации Which протестировали на безопасность 28 игрушек с AliExpress, Amazon, eBay и Wish. В результате 12 товаров не прошли проверку по одному или сразу нескольким параметрам: всего эксперты насчитали 50 нарушений.

Часть проверенных игрушек не соответствовали межгосударственным стандартам, принятым в том числе и в России: EN 71-1-2014 «Игрушки. Требования безопасности» и IEC 62115-2014 «Игрушки электрические. Требования безопасности». Среди критических несоответствий: длинные шнурки и проводки, которые могут стать причиной удушья; ломкие детали, о которые можно пораниться; мелкие детали, магнитики и батарейки, которые ребенок может проглотить. После расследования Which 12 опасных игрушек, которые не прошли проверку, были удалены AliExpress, Amazon, eBay и Wish.

По данным Роспотребнадзора, доля некачественных товаров для детей за 7 лет выросла вдвое — в 2013 году из проверенных товаров (одежда, обувь, посуда, коляски и т. д.) 5,2 % были признаны некачественными, а в 2019 — уже 10,3 %. При этом доля игрушек, не соответствующих нормативным требованиям, в 2019 году составила 7,3 %, а в 2013 — 6,8 %. На импортные товары в общем объеме забракованной продукции пришлось в среднем 40 %.

Комиссия США по безопасности потребительских товаров отозвала более 400 игрушек, которые представляли угрозу жизни и здоровья детей за период с 2008 по 2014 год, что привело к значительным расходам производителей, розничных продавцов и потребителей.

По данным отчета Комиссии по безопасности потребительских товаров США, в 2013 году было вылечено более 250 тысяч травм, связанных с игрушками. Из них 73 % травм приходилось на детей младше 15 лет, 69 % — на детей младше 12 лет, и 33 % — на детей младше 5 лет.

Примеры

Гидрогелевые шарики (2018)

В мае 2018 года врачи республиканской детской клинической больницы в Уфе спасли годовалого мальчика: ребенок едва не погиб, проглотив большое количество гидрогелевых шариков. Ребенку провели две операции, почти месяц он пролежал в больнице. В апреле 2018 года ситуация повторилась: московские врачи спасли жизнь годовалой девочке, у которой отказала пищеварительная система из-за того, что она проглотила гидрогелевые шарики.

Перепродажа пиротехники, купленной через интернет (2019)

В 2020 году в Минске задержали 13-летнего мальчика, который втайне от родителей купил в интернете петарды и продавал их с наценкой около магазина. На него пожаловались прохожие. В отношении родителей мальчика составили административный протокол за невыполнение обязанностей по воспитанию детей, а с ним сотрудники инспекции по делам несовершеннолетних провели профилактическую работу.

Токсичные лизуны (2018)

В 2018 году в Пензе изъяли партию популярных у школьников лизунов с содержанием запрещенного токсичного вещества дибутилфталата. Игрушки содержали маслянистую жидкость, которая может оказывать негативное влияние на центральную и периферическую нервную систему ребенка.

Источники

1. Афанасьева Эльмира. «Современные тенденции развития российского рынка детских товаров». Управление экономическими системами: электронный научный журнал №2 (74) (2015)
2. Даревская Виктория. «Что грозит за взрыв петард в Беларуси». Минск-Новости (2020), minsknews.by/dumal-koresh-idet-napugat-hotel-a-tut-vy-chto-grozit-za-vzryv-petard-v-belarusi
3. Крайнов Павел. «В Уфе врачи спасли ребенка, проглотившего гидрогелевый шарик». Комсомольская правда (2018), www.ufa.kp.ru/online/news/3107418 .
4. Перцева Евгения. «Опасные игры: доля некачественных детских товаров выросла вдвое». Известия (2020), iz.ru/1036122/evgeniia-pertceva/opasnye-igry-dolia-nekachestvennykh-detskikh-tovarov-vyrosla-vdvoe
5. Солдатова Г. У. и др. «Цифровое поколение России: компетентность и безопасность». Litres (2020)
6. «Врачи Филатовской больницы борются за жизнь годовалой девочки». «Вести», Россия 1 (2018), filatovmos.ru/feedback2/14-news/312-shariki.html
7. «Доигрались. Почему российские власти решили ужесточить контроль за лизунами, спиннерами и другими игрушками». Известия (2018), https://iz.ru/727444/ekaterina-korinenko/doigralis

8. «Новое поколение интернет-пользователей: исследование привычек и поведения российской молодежи онлайн». Google and Ipsos (2017)
9. «Новое поколение: исследование детей и подростков». Ipsos (2020)
10. Suk, William A. et al. «Environmental hazards to children's health in the modern world». Mutation Research/Reviews in Mutation Research (2003): 235-242
11. Warentest, Stiftung. «Unsichere Kinderprodukte». (2018)
12. Winkler, Matt, et al. «Toy safety surveillance from online reviews». Decision support systems 90 (2016): 23-32
13. «American Academy of Pediatrics: children, adolescents and television». Pediatrics 107.2 (2001): 423-426
14. «Impact of media use on children and youth». Paediatr Child Health (2003)
15. «Safety alert: Serious button battery and magnet dangers in online marketplace toys». Which (2021), https://www.which.co.uk/news/2021/08/safety-alert-serious-button-battery-and-magnet-dangers-in-online-marketplace-toys/
16. «Safety in Educational Toys». Edx Education (2021), https://edxeducation.com/safety-in-educational-toys/
17. «Toy Recall Statistics». United States Consumer Product Safety Commission (2015), http://www.cpsc.gov/en/Safety-Education/Toy-Recall-Statistics/
18. «Toy-Related Deaths and Injury Calendar». United States Consumer Product Safety Commission (2015), http://www.cpsc.gov/Global/

6. Продвинутые методики маркетинга

Передовые маркетинговые стратегии помогают компаниям выстраивать отношения с клиентами, в том числе с детьми.

Дети — желанная цель для маркетологов. Компании применяют сложные алгоритмы для нацеливания рекламы на детей в социальных сетях и играх, например, датамайнинг и профилирование. При этом персональные данные и профили детей доступны для покупки бизнесом.

Каждый четвертый ребенок покупает на карманные деньги то, что ему рекламируется. При этом даже если дети не могут самостоятельно приобретать товары, они способны убеждать своих родителей совершать такие покупки.

Специфика риска

По данным Statista, в 2020 году в мире было потрачено 378 млрд долларов на цифровую рекламу, а в 2021 эта сумма выросла до 455 млрд долларов.

Ребенок — это потребитель, который тратит свои карманные деньги, влияет на покупки родителей, а в будущей взрослой жизни тратит уже собственные деньги на любимые бренды. Например, только в США дети до 12 лет тратят в среднем 50 млрд долларов в год, подростки — в три раза больше. Кроме того, дети побуждают родителей приобретать товары почти на 600 млрд долларов в год.

В последнем десятилетии реклама совершила несколько серьезных шагов вперед. Раньше она больше вредила детской самооценке, увеличивала потребление табака и алкоголя, приводила к расстройствам питания и нездоровому отношению к покупкам, чем сейчас. Сегодня компании применяют сложные алгоритмы для нацеливания рекламы на детей в социальных сетях и играх с ограниченным регулированием. Персональные данные детей продаются между компаниями, а профилями детей торгуют как товарами.

Датамайнинг и профилирование

Технологии датамайнинга (интеллектуального анализа данных) создают подробные демографические и поведенческие профили детей и молодежи в интернете. Затем эта информация используется для документирования современных тенденций на молодежных рынках. Интеллектуальный анализ данных — это процесс сбора «совокупной», а не «личной» информации.

Процесс получения потребительской информации для коммерческого прогнозирования вызывает ряд этических проблем, включая вопросы конфиденциальности и владения интеллектуальной собственностью в отношении информации и контента, не идентифицирующих личность.

Профилирование ребенка может иметь серьезные последствия для всей его последующей жизни, с учетом его неспособности от своего имени давать свободное, конкретное и информированное согласие при сборе личных данных. Методы профилирования, выявляя взаимосвязи между конфиденциальными и другими данными, могут привести к созданию новых чувствительных данных. Недостаточная прозрачность или даже просто «невидимость»

профилирования граждан и отсутствие точности, которая может проистекать из автоматического применения заранее установленных правил, создает значительный риск для прав и свобод человека.

Предиктивная аналитика

Предиктивная или прогнозная аналитика — это набор методов интеллектуального анализа данных, которые позволяют прогнозировать будущее поведение исследуемых объектов. Предиктивная аналитика, как правило, базируется на автоматизированной обработке данных большого объема.

Предиктивная аналитика определяет новые маркетинговые возможности с помощью трех различных моделей:

1. модель склонности — предвидение аналитическими платформами вероятности совершения покупки конкретным покупателем;
2. модель совместной фильтрации — предугадывание типов продуктов и услуг, которые клиент с большой вероятностью купит, на основе истории покупок;
3. кластерная модель — разделение клиентской базы на различные нишевые кластеры, например, кластеризация на основе бренда или продукта, кластеризация по поведению.

Таргетинг в социальных сетях

Таргетинг — механизм, при помощи которого из всех интернет-пользователей можно выделить только ту аудиторию, которая соответствует определенным критериям, и донести до нее рекламную информацию.

Для использования социальных сетей (Facebook*, Instagram*, Snapchat, TikTok и т. д.) необходимо создать профиль. При этом каждый пользователь соглашается на то, чтобы его данные собирались и предоставлялись рекламодателям. По мере увеличения активности пользователей компании узнают о привычках и предпочтениях аудитории, что создает ценность для рекламодателей. Объем данных, генерируемых миллиардами людей, означает, что модели поведения поддаются обнаружению и, следовательно, в определенной степени предсказуемы.

Реклама, ориентированная на расходы родителей на детей

Маркетологи, работающие с детской аудиторией до 14 лет, говорят, что товары играют важную роль в общении со сверстниками, будь то компьютерная игра, сайт для скачивания музыки или новая модная игрушка — обладание товаром становится ключом к признанию и популярности. Дети предпочитают те товары, кампания по продвижению которых задействует как можно больше органов чувств. Так, чтобы стать популярным, герой комикса должен появиться в фильме, мультсериале, игре и на прилавке с игрушками.

Детская реклама использует наивность детей. Из-за того, что большинство детей верят в то, что они видят и слышат, они также считают, что продукт или услуга действительно обеспечат преимущества и удовольствия, которые обещает реклама, даже если это нечто абсолютно нереальное и невозможное для реализации.

---

* Признаны экстремистскими организациями, деятельность которых запрещена на территории Российской Федерации

Для детей реклама — это, прежде всего, простейшая модель знакомства с окружающей средой. При этом дети и подростки воспринимают информацию гораздо острее и критичнее.

Распространенность

В ходе исследования, проведенного учеными из Института человека РАН и Московского государственного психолого-педагогического университета, было выявлено, что с возрастом усиливается критическое отношение детей к рекламе, однако, дети в раннем возрасте положительно относятся к рекламе, доверяют ей и любят ее смотреть.

В группе дошкольного возраста больше половины детей положительно относятся к рекламе. В младшем школьном возрасте таких детей оказалось 38 %, среди детей 11-12 лет — только 18 %, а детям старшего возраста реклама категорически не нравится.

Самый большой процент доверия рекламе у дошкольников — 50 %. Отношение детей из младших классов более осознанно и критично, доверяют рекламе только 23-30 % детей, а больше половины — не доверяют вовсе.

Реклама для детей все чаще перемещается с телевидения в интернет. Это соответствует меняющимся потребительским привычкам детей, которые проводят время в интернете.

В то время как компании получают прибыль со своих рекламных кампаний, дети, семьи и общество расплачиваются за это.

Согласно данным опроса QIWI и Ipsos Comcon, дети в возрасте от 4 до 15 лет в совокупности получают почти 800 млн рублей на карманные расходы в неделю. Ежегодные траты российских детей составляют 5-6 млрд долларов. При этом 26 % детей покупают на карманные деньги то, что им рекламируется.

Воздействие рекламы связано с покупкой нездоровых продуктов питания семьями с маленькими детьми. Кроме того, из-за влияния рекламы на выбор у детей часто наблюдаются проблемы с избыточным весом и ожирением. С 1975 по 2016 год число детей и подростков, страдающих ожирением, увеличилось в 11 раз.

Среди детей в возрасте 5-7 лет в Бразилии, Китае, Индии, Нигерии и Пакистане 68 % опрошенных смогли идентифицировать хотя бы один логотип марки сигарет. В Китае это число достигает 86 %.

В Великобритании каждый восьмой ребенок в возрасте 11-16 лет следит за игорной компанией в социальных сетях, в то время как азартные игры связаны со стрессом, срывом учебы и конфликтом в общении с родителями.

Примеры

Реклама наркотиков в Instagram* (2021)

В декабре 2021 года Tech Transparency Project провела исследование, связанное с продажей наркотиков в Instagram*. Политика социальной сети запрещает покупку и продажу наркотиков, однако, исследователям удалось обнаружить, что это правило не соблюдается. Для целей эксперимента было создано несколько аккаунтов несовершеннолетних пользователей в

возрасте 13-17 лет, а затем предпринятыпопытки найти аккаунты, через которые можно приобрести наркотические средства.

Instargam* не только позволил подросткам искать нелегальные наркотики, алгоритмы платформы помогли несовершеннолетним аккаунтам напрямую связаться с наркоторговцами, продающими различные виды запрещенных веществ.

Торговая сеть Target (2012)

В 2012 году американская торговая сеть Target узнала о беременности школьницы раньше, чем сама девушка. Произошло это благодаря используемым в данном магазине алгоритмам прогнозирования поведения покупателей. На основе анализа покупок девушку отнесли к группе беременных, поэтому торговая система стала посылать ей соответствующие купоны.

Данный пример показывает, насколько предсказуемы и прогнозируемы наши действия и покупательские привычки. Это событие заставило общественность обратить внимание на то, каким количеством информации владеет ритейлер, и задаться вопросом о правомерности использования этих данных.

Cambridge Analytica (2016)

После выборов в США 2016 года выяснилось, что компания Cambridge Analytica занималась разработкой политической таргетированной рекламы и использовала базу данных о 50 млн американцев, чтобы помочь кандидату в президенты Дональду Трампу выиграть выборы. Использование Facebook* и больших данных позволило компании составлять рекламные сообщения согласно особенностям каждого пользователя. Компания также собирала данные о пользователях Facebook* с помощью стороннего приложения, которое задавало невинные вопросы, но на самом деле было нацелено на профилирование пользователей.

Федеральная торговая комиссия США оштрафовала Facebook* на 5 млрд долларов. Доверие к соцсети значительно снизилось, общественность стала обсуждать этичность такого подхода к кампаниям политических кандидатов. Основатель и глава Facebook* Марк Цукерберг и профессор психологии Кембриджского университета Александр Коган, находившиеся в центре скандала, предстали перед Конгрессом США, когда дело дошло до высших инстанций.

Источники

1. Авдеева Наталья и Наталья Фоминых. «Влияние телевизионной рекламы на детей и подростков» (2003)
2. Брускин Сергей. «Модели и инструменты предиктивной аналитики для цифровой корпорации». (2017)
3. Логачев А. «AdTech Market Overview» (2019)
4. Мустафина Екатерина. «Влияние рекламы на психику детей и подростков». Вопросы российской юстиции 14 (2021): 7-19
5. Селизарова Варвара. «На что дети тратят карманные деньги». РБК +1 (2017), https://plus-one.rbc.ru/society/na-chto-deti-tratyat-karmannye-dengi
6. Шкор О. Н. и А. И. Головач. «Предсказательная аналитика в маркетинге» (2021)
7. «На что способны Big Data или супер-кейс сети Target». Retail.ru (2015), https://www.retail.ru/cases/na-chto-sposobny-big-data-ili-super-keys-seti-target/

8. «Рекомендация CM/Rec 13 Комитета министров странам-членам по вопросам защиты частных лиц в связи с автоматизированной обработкой персональных данных в контексте профилирования граждан» (2010)
9. Abarca-Gómez et al. «Worldwide trends in body-mass index, underweight, overweight, and obesity from 1975 to 2016» (2017)
10. Buchanan, L. «Advanced Marketing Strategies to Add Value to Your Business» (2021)
11. Chung, Grace and Sara M. Grimes. «Data Mining the Kids: Surveillance and Market Research strategies in children's online games» (2005)
12. Feldman, S. «Digital Advertisers Increasingly Target Kids» (2019)
13. Rosenbloom, Maxie. «Request for Public Comment on the Federal Trade Commission's Request for Comments Regarding Topics to be Discussed at Dark Patterns Workshop» (2021)
14. «Digital advertising spending worldwide from 2019 to 2024». Statista (2021)
15. «Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You». Time (2018)
16. «Kids for Sale: Online Advertising and the manipulation of children». Global Action Plan (2020)
17. «Protecting children from harmful marketing practices». WHO-UNICEF-Lancet Commission (2020)
18. «Why advertising is bad for children». Projeto Criança e Consumo (2009)
19. «Xanax, Ecstasy, and Opioids: Instagram Offers Drug Pipeline to Kids». Tech Transparency Project (2021)

7. Темные паттерны

Темные паттерны — это тонкие психологические уловки и дизайнерские решения, которые подталкивают пользователей на выполнение определенных действий.

Существует множество методов манипулятивного дизайна, которые подталкивают пользователей сделать то, чего в противном случае они бы не стали делать. Эти методы получили широкое распространение в последние годы, и в настоящее время компании широко применяют их на детскую аудиторию.

Воздействие темных паттернов усугубляется тем, что дети не могут защитить себя от них, так как не обладают необходимыми когнитивными и аналитическими способностями. Они уязвимы, склонны к импульсивному поведению, легко формируют отношения с персонажами, поддаются влиянию вознаграждений и статусов, при этом у них еще не сформировано зрелое понимание о ценности денег и недостаточно высокий уровень финансовой грамотности.

Специфика риска

Темные паттерны намеренно подталкивают пользователей к определенным действиям, поощряя постоянное совершение покупок. Игры и приложения могут использовать UI/UX-решения[6], чтобы побудить детей продолжать пользоваться приложением и/или оплачивать покупки.

Ученые, занимающиеся исследованием данной проблемы, связывают распространение темных паттернов с популярностью онлайн-игр. Для того чтобы монетизировать игру, разработчики применяют четыре основные механизма: реклама внутри игрового процесса, покупки в игре, загружаемый контент, подписка.

Создатели развлекательного контента используют темные паттерны, чтобы дети и подростки больше играли и тратили деньги в приложении. Наиболее популярные виды темных паттернов в онлайн-играх и приложениях для детей объединяют в следующие группы: синдром упущенной выгоды (FOMO), социальный аспект и статус персонажа, бесконечный поток контента, премиальные игровые валюты, сложный интерфейс.

Синдром упущенной выгоды. Компании используют темные паттерны, чтобы эксплуатировать детский страх упустить что-либо. Это реализуется благодаря таймерам, ограниченным по времени заданиям и игровым миссиям, эксклюзивным или сезонным предложениям и товарам.

Социальный аспект и статус персонажа. Ребенок может считать, что владение редкими игровыми предметами повышает его престиж среди друзей, и аналогичным образом может испытывать давление, когда друзья приобретают себе дорогостоящие предметы. Также дети могут испытывать беспокойство по поводу пропущенных игровых событий, за участие или победу в которых игрокам присваивается новый статус.

Бесконечный поток контента. Может проявляться в моделях, когда ребенок развивается в игре за счет времени, затраченного на повторяющиеся задачи, дополнительного контента или возрастающих уровней сложности после легкого старта. Это заставляет ребенка чувствовать, что он должен находиться в игре постоянно, не отвлекаясь на другие дела.

---

[6] UI (User Interface) — пользовательский интерфейс. UX (User Experience) — пользовательский опыт.

Премиальные игровые валюты. Премиальные игровые валюты используются, чтобы скрыть ценность потраченных денег. Кроме того, премиальные игровые валюты, как правило, продают оптом, побуждая детей покупать большее количество за один раз. Так, например, внутриигровая валюта в игре Dragon City — драгоценные камни, а в игре Fortnite — В-баксы (V-Bucks).

Сложный интерфейс. Даже когда ребенок не хочет совершать покупки в приложении, темные паттерны могут перенаправлять его обратно в раздел покупок. Вариант отказаться от покупки может быть незаметен или слишком сложен. Например, разработчики пользовательского интерфейса для игры Fortnite изменили внешний вид кнопки «Отменить покупку», чтобы свести к минимуму ее видимость и побудить пользователей переходить к этапу, на котором они не смогут отменить потенциально нежелательные покупки.

Исследование 2018 года показало, что треть из 135 приложений на базе операционной системы Android, которыми пользуются дети, побуждали их оценивать приложение в магазине Google Play, а 14 % — делиться информацией в социальных сетях. Такими действиями дети предоставляют приложениям широкие права доступа для использования информации из социальных сетей. Кроме того, параметры конфиденциальности в многопользовательских играх часто по умолчанию используют настройки, раскрывающие личные данные.

Парасоциальные отношения

Дети часто развивают доверительные отношения с игровыми персонажами и ведут себя так, как будто у этих персонажей есть реальные мысли и чувства. Подталкивая детей совершать покупки для удовлетворения эмоциональных потребностей персонажей, у которых на самом деле нет эмоций, компаниям становится проще использовать этих персонажей, чтобы манипулировать детьми.

Стоит отметить, что перечисленные темные паттерны, как правило, используются вместе и дополняют эффект друг от друга, при этом они используются не только в играх, но и на сайтах, в приложениях, онлайн-магазинах. Воздействие темных паттернов усугубляется тем, что дети не могут защитить себя от них, так как не обладают необходимыми когнитивными и аналитическими способностями.

Так как дети зачастую пользуются бесплатными приложениями и играми, вероятность того, что они столкнутся с темными паттернами, увеличивается. Это связано с тем, что монетизация бесплатных приложений происходит за счет рекламы, внутриигровых покупок и использования или продажи персональных данных пользователей.

Распространенность

Исследование, в ходе которого было проанализировано 11 000 самых популярных сайтов, выявило 1818 темных паттернов на 1254 веб-сайтах. Поскольку 95 % детей имеют доступ к смартфону и проводят значительную часть своего времени, пользуясь мобильным телефоном, риск столкновения с темными паттернами очень актуален. Несовершеннолетние легче взрослых поддаются манипулированию, поэтому темные паттерны адаптируют под детскую аудиторию.

Одним из видов внутриигровых покупок могут быть лутбоксы.[7] Аналогично азартным играм, люди рискуют деньгами в зависимости от случайного исхода события — лутбоксы покупают за реальные деньги, не зная, что именно попадется внутри. По данным на 2020 год, 54 % лучших игр в магазине Google Play и 34 % лучших игр в магазине Steam использовали механику лутбоксов. Особенное беспокойство вызывает то, что 94 % этих игр доступны для детей от 12 лет, а подверженность азартным играм в детстве предсказывает проблемы с азартными играми в дальнейшей жизни.

Эффект от применения темных паттернов напрямую отражается на прибыли компании, которая их использует. Так, например, в Electronic Arts объявили, что 74 % доходов компании (6,19 млрд долларов) за 2021 год приходится на загружаемый контент, микротранзакции и покупки внутри игр, при этом фактические продажи игр приносят только оставшиеся 26 %.

Примеры

Ребенок потратил на игру 16 тысяч долларов (2020)

Шестилетний мальчик из американского города Уилтон, штат Коннектикут, потратил 16,2 тысяч долларов с кредитной карты матери, покупая дополнения к своей любимой компьютерной игре Sonic Forces.

Когда женщина получила счет, она подумала, что стала жертвой мошенничества и подала заявление в банк. В октябре банк подтвердил, что счета были выставлены правомерно и порекомендовали обратиться в компанию Apple. К тому моменту установленный Apple 60-дневный срок возврата платежей прошел.

В результате семья не смогла выплатить ссуду за жилье. Компания Apple отказалась вернуть деньги, мотивировав это тем, что родители сами виноваты, что проигнорировали настройки родительского контроля.

Мать ребенка сравнила одержимость компьютерными играми с пристрастием к наркотикам, добавив, что эти игры созданы, чтобы заставлять детей тратить деньги на дополнения. Также она отметила, что ребенок не понимал, что деньги настоящие, так как думал, что тратит виртуальные деньги.

Ребенок купил виртуальные ресурсы за 320 тысяч рублей (2020)

Житель подмосковного города Ногинск столкнулся с пропажей крупной суммы со своего банковского счета. Оказалось, что его собственный несовершеннолетний сын потратил 320 тысяч рублей на микротранзакции в популярной аниме-игре Bleach: Immortal Soul. На эти деньги он купил виртуальные ресурсы, необходимые для быстрого развития.

Отец ребенка решил вернуть деньги: обратился в Google и даже подал на компанию в суд. Однако его претензия так и не была рассмотрена в суде, потому что стороны пришли к компромиссу и урегулировали спор.

Источники

[7] Лутбокс — виртуальный предмет в компьютерных играх, при использовании которого игрок получает случайные виртуальные артефакты различной ценности и назначения, называемые добычей.

1. Седых И. А. «Индустрия компьютерных игр». НИУ ВШЭ (2020)
2. «Российский школьник потратил сотни тысяч родительских денег на игру». CNews.ru (2020), www.cnews.ru/news/top/2020-12-01_rossijskij_shkolnik_potratil
3. Bloemen, Noor and David De Coninck. «Social Media and Fear of Missing Out in Adolescents: The Role of Family Characteristics». Social Media and Society 6.4 (2020)
4. Brunick, Kaitlin L., et al. «Children's future parasocial relationships with media characters: The age of intelligent characters». Journal of Children and Media 10.2 (2016): 181-190
5. Coulson, Josh. «Just 26 % of EA's Revenue Now Comes From Game Sales». The Gamer (2021), https://www.thegamer.com/26-ea-revenue-game-sales/
6. Crone, Eveline A. and Elly A. Konijn. «Media use and brain development during adolescence». Nature communications 9.1 (2018): 1-10.
7. Di Geronimo, Linda, et al. «UI dark patterns and where to find them: a study on mobile applications and user perception». Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (2020)
8. Jacobs, DF. «Juvenile gambling in North America: An analysis of long term trends and future prospects». J Gambl Stud. (2000): 119–152
9. Jourová, V. «The impact of online marketing on children's behaviour». European Commission (2016)
10. Lewak, Doree. «This 6-Year-Old Racked up $16K on Mom's Credit Card Playing Video Games». New York Post (2020), https://nypost.com/2020/12/12/this-6-year-old-racked-up-over-16k-on-his-moms-credit-card/
11. Mathur, Arunesh, et al. «Dark patterns at scale: Findings from a crawl of 11K shopping websites». Proceedings of the ACM on Human-Computer Interaction 3.CSCW (2019): 1-32
12. Meyer, Marisa, et al. «Advertising in young children's apps: A content analysis». Journal of developmental & behavioral pediatrics 40.1 (2019): 32-39
13. Rieger, Sebastian and Caroline Sinders. «Dark Patterns: Regulating Digital Design». SNV (2020)
14. Rosenbloom, Michael. «Dark patterns». (2021)
15. Zendle, David, et al. «The prevalence of loot boxes in mobile and desktop games». Addiction 115.9 (2020): 1768-1772
16. «Connecticut Boy, 6, Racked up $16K Bill on His Mom's Credit Card Playing Video Games on Her IPad». Daily Mail (2020), https://www.dailymail.co.uk/news/article-9048605/Connecticut-boy-6-racked-16K-bill-moms-credit-card-playing-video-games-iPad.html
17. «What Is Freemium?» Investopedia (2021), www.investopedia.com/terms/f/freemium.asp

8. Онлайн-мошенничество

Интернет-сервисы или программное обеспечение с доступом в интернет может применяться для обмана пользователей.

В связи с тем, что дети и подростки наиболее подвержены внушению, а их психоэмоциональные особенности находятся на стадии созревания, они являются одной из наиболее уязвимых категорией жертв для онлайн-мошенников.

Последствия онлайн-мошенничества имеют как финансовые, так и социально-психологические последствия, включающие в себя стресс, ощущение разочарования и несправедливости.

Специфика риска

Онлайн-мошенничество является разновидностью мошенничества, а ключевой особенностью является то, что преступления происходят через взаимодействие в интернете. Эта преступная деятельность преследуется законом независимо от места совершения — офлайн или в интернете.

К видам онлайн-мошенничества можно отнести фишинг, лотереи, подарочные акции, спам с заманчивыми предложениями, поддельные кошельки платежных систем и всевозможные их комбинации.

Дети регулярно сталкиваются с фишингом: в социальных сетях или на электронную почту им могут приходить сообщения о выигрыше дорогого приза или возможности поучаствовать в конкурсе, чтобы получить награду. Также ребенок может нажать на поддельные всплывающие окна, предупреждающие о возможных вирусах и вредоносных программах. Это выглядит убедительно, поэтому дети, руководствуясь намерением защитить компьютер, переходят по вредоносным ссылкам.

Дети сталкиваются с мошенничеством и в онлайн-играх. Это может быть реализовано путем перенаправления игроков на сторонние сайты, атак на IP-адреса игроков, фишинга, скачивания поддельных мобильных версий популярных онлайн-игр. Преступники обманным путем получают доступ к учетной записи ребенка, после чего похищают виртуальные средства и деньги из онлайн-кошелька.

Последствия онлайн-мошенничества имеют как финансовое, так и социально-психологическое проявление, включающее в себя стресс, ощущение разочарования и несправедливости.

Распространенность

В 2017 году более миллиона детей в возрасте до 17 лет были зарегистрированы в качестве жертв кражи личных данных только в США, что привело к убыткам примерно в 2,6 млрд долларов. Согласно исследованию Social Catfish, число лиц в возрасте до 20 лет, ставших жертвами онлайн-мошенничества, выросло на 156 % за последние 3 года.

Исследование 2018 года, в ходе которого было опрошено почти 1000 респондентов разных возрастов, показало, что с некоторыми видами онлайн-мошенничества особенно часто сталкиваются несовершеннолетние жертвы.

Среди всех респондентов, которые сталкивались с мошенничеством на международном рынке Forex, фондовых или валютных биржах, насчитывается 36,5 % несовершеннолетних. Также дети и подростки составляют одну треть от тех, кто покупал программное обеспечение или сим-карту для мобильного телефона, позволяющие «бесплатно» использовать услуги связи. Среди жертв, столкнувшихся с сообщениями о помощи в переводе денег от лица друзей и знакомых, несовершеннолетние составляют 33,3 %. При этом 32,3 % всех респондентов, у которых была похищена предоплата за товар, продаваемый в социальных сетях или на специализированных сайтах, не достигли 18 лет. С фишингом столкнулись 26,6 % детей от общего числа опрошенных жертв. А предложения перевести деньги на «секретный» электронный кошелек, который должен увеличить сумму переведенных средств, получила группа людей, на одну четвертую состоявшая из детей и подростков (25 %).

Некоторые из перечисленных видов онлайн-мошенничества связаны с желанием получить материальные блага быстро и/или бесплатно. Такая тактика злоумышленников по отношению к детям и подросткам находит объяснение с точки зрения психологии. Отсутствие доступных способов заработка, развитый уровень пользования интернетом, а также незнание или намеренное игнорированием мер информационной безопасности делают несовершеннолетних привлекательным объектом для подобных мошеннических схем.

По результатам опроса среди 45 000 детей в возрасте от 6 до 18 лет стало известно, что 13 % детей не знают, как правильно общаться в сети, а 25 % детей не умеют бороться с негативными эмоциями в интернете и противостоять давлению.

24 % из 345 опрошенных израильских детей и подростков высказались за заблаговременное принятие мер для предотвращения рисков и осознанный подход к использованию интернета. Участники исследования также заявили, что пользователь сам несет ответственность за свою безопасность в сети. Кроме того, 19 % подчеркнули важность конкретных мер, таких как блокировка опасных веб-сайтов и защита компьютера антивирусным программным обеспечением, а каждый пятый (21 %) указал на необходимость повышения осведомленности и просвещения по вопросам безопасности среди детей и подростков.

Примеры

Онлайн-мошенничество в Steam (2021)

Семнадцатилетний подросток рассказал о двух случаях, в которых стал жертвой онлайн-мошенников в игре. В десятилетнем возрасте мальчик нашел программу для «накрутки» вещей в компьютерной игре CS:GO. Эта программа полностью имитировала экран входа в онлайн-сервис цифрового распространения компьютерных игр и программ Steam. Юноша ввел свои данные от аккаунта на фишинговом сайте, после чего их похитили злоумышленники и перепродали дорогостоящие игровые атрибуты.

Отмывание денег (2021)

Семнадцатилетняя Шарлотта оказалась жертвой мошенничества с отмыванием денег. Подруга Шарлотты Сара сказала, что ей нужно перевести деньги другому человеку, а банк не позволяет это сделать. Затем Сара перевела деньги Шарлотте и попросила ее отправить их конечному адресату.

Но эти деньги не принадлежали Саре — они были украдены наличными, зачислены на счет Сары, а затем Шарлотты, чтобы «отмыть» их, прежде чем они попадут на счет мошеннику. Оказалось, что незадолго до этого Сара откликнулась на объявление о работе, которая заключалась в передаче полученных от третьего лица денег другому человеку. В этой цепочке Шарлотта стала невольным сообщником.

В течение нескольких часов банковский счет Шарлотты был заморожен, а ее кредитный рейтинг — понижен.

Источники

1. Анцупов Игорь и др. «О проблемах повышения цифровой грамотности молодежи: генезис проблемы, подходы психолого-педагогической науки». Проблемы современного педагогического образования 67-4 (2020): 31-33
2. Белицкий В. Ю. «Распространенные виды мошенничеств в сети интернет». Актуальные проблемы современности 2 (2020): 31-36
3. Нашилов Егор. «Байки из Steam: как разводят геймеров». Kaspersky (2021), https://www.kaspersky.ru/blog/tales-from-steam/30090/
4. Никитина Ирина. «Финансовое мошенничество в сети Интернет». Вестник Томского государственного университета. № 337 (2010): 122–124.
5. Соловьев В. С. «Мошеннические действия в социальном сегменте сети Интернет (криминологическое исследование по результатам интернет-опроса пользователей)». Известия Юго-Западного государственного университета. Серия: История и право 8.3 (2018): 100-108.
6. Токарев Н. В. «Использование психологического воздействия при совершении мошенничества в условиях цифровизации экономики». Молодежная наука: тенденции развития № 1 (2021): 48-52
7. «Мошенничество в играх во время пандемии коронавируса: как защитить себя и свою семью». Kaspersky, https://www.kaspersky.ru/resource-center/threats/coronavirus-gaming-scams
8. Grant, K. «Child identity theft is a growing and expensive problem». CNBC (2018), https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html
9. Orcutt, Ashley Mae. «State of Internet Scams». (2021), https://socialcatfish.com/blog/state-of-internet-scams-2021/
10. Zilka, Gila Cohen. «Awareness of eSafety and potential online dangers among children and teenagers». Journal of Information Technology Education: Research 16 (2017)
11. «Internet fraud — seniors and teenagers». Citywide banks, https://www.citywidebanks.com/sites/heartland/files/1232_18_Internet_Fraud_Retail.pdf
12. «Why financial scams may be the biggest cyber-threat to your children». Newscentre.Vodafone (2021), https://newscentre.vodafone.co.uk/smart-living/digital-parenting/why-financial-scams-may-be-the-biggest-cyber-threat-to-your-children/

Группа 3. Личностная атака, психологическое насилие

К этой группе относятся риски, конечная цель которых — нанести моральный, физический или иной ущерб конкретному ребенку, например: кибербуллинг, сталкинг, груминг и сексуальные домогательства.

В случае наступления этих рисков, жертвой становится конкретный ребенок, а злоумышленник проявляет целенаправленную агрессию в его сторону или предпринимает попытки использовать ребенка в корыстных и противоправных целях.

9. Кибербуллинг

Кибербуллинг подразумевает повторяющиеся эпизоды агрессивного поведения, направленные на то, чтобы напугать, унизить или разозлить человека.

Такая форма поведения встречается в социальных сетях, мессенджерах, игровых платформах и других онлайн-площадках. Кибербуллинг может совершаться и детьми, и взрослыми.

Кибербуллинг негативно влияет на поведение, психоэмоциональное и физическое здоровье жертвы. Изменения в эмоциональном состоянии характеризуются резкой переменой настроения в сторону негативных эмоций.

Специфика риска

Определение кибербуллинга варьируется от работы к работе. Метаанализ, проведенный в 2020 году, установил, что лишь 72 % исследований включали объяснение термина или определение концепции. Более того, лишь 50 % работ из выборки включали в себя термин «кибербуллинг», остальные использовали синонимы.

Проявления этого феномена в офлайн-среде широко варьируются и сильно зависят от культуры, но у него есть давно установленные кросс-культурные критерии: намерение навредить, регулярность, неравенство в силах обидчика и жертвы.

Эти критерии также во многом характеризуют кибербуллинг. Травля в интернете может переходить в офлайн-взаимодействия, а насилие в реальной жизни может дополняться кибербуллингом.

Обидчики в киберпространстве более жестоки из-за того, что они анонимны — их сложнее выявить и привлечь к ответственности. Кроме того, они не видят жертву, а поэтому не видят результатов своих действий, что усугубляет ситуацию.

Последствия кибербуллинга

Кибербуллинг оказывает влияние на эмоциональное состояние, психологическое здоровье, поведение и физическое здоровье жертвы. Изменения в эмоциональном состоянии характеризуются резкой переменой настроения в сторону негативных эмоций — злости, раздражительности, уныния, боязливости, одиночества. Конкретный эмоциональный эффект зависит от ребенка.

Влияние на психологическое здоровье характеризуется снижением внимательности и академической успеваемости. Возможно возникновение депрессии, нездорового интереса к суициду. Падают самооценка и уверенность в себе, могут возникнуть пищевые расстройства, например, булимия или анорексия.

У жертвы кибербуллинга увеличивается вероятность злоупотребления алкоголем и наркотиками. Могут возникать прогулы или внезапное отвращение к телефонам, компьютерам. Наиболее тревожными результатами являются нанесение себе повреждений и в крайних случаях — суицид.

С точки зрения физического здоровья могут возникать недосыпы, головные боли, расстройства психосоматического характера. Ребенок переживает постоянный стресс, что приводит к нарушениям в работе организма.

Распространенность

Средняя осведомленность о кибербуллинге по миру составляет 75 %. Россия заняла 26 место из 29 стран с показателем в 56 % за 2018 год.

В 2016 году 46 % граждан РФ были осведомлены о проблеме, а в 2011 — всего 35 %.
В России в 2012 году присутствовали существенные проблемы в вопросе распространенности кибербуллинга в сравнении с остальным миром. 49 % детей в возрасте 8-17 лет становились жертвами издевательств в онлайне, а 33 % сами занимались буллингом своих сверстников в интернете.

По данным британского НКО Ditch The Label, которое проводит ежегодные опросы тысяч подростков по теме буллинга онлайн и офлайн, в 2020 году 27 % кейсов травли включали в себя кибербуллинг.

Опрос, проведенный в США среди учеников средних и старших школ, показал: 38,7 % девочек и 34,1 % мальчиков становились объектами кибербуллинга хотя бы раз в своей жизни.
Несмотря на изменения в самих цифрах между исследованиями, одна тенденция проявляется в течение всего времени: девочки чаще подвергаются кибербуллингу, чем мальчики. Мальчики чаще выступают обидчиками.

В 2015 году 28 % детей в возрасте 10-18 лет были жертвами кибербуллинга хотя бы раз в жизни. Свидетелями кибербуллинга были 87 % опрошенных, при этом 4 % таких случаев приводили к дракам в реальности. Также было выявлено, что 16,2 % опрошенных выступали провокаторами.
По данным того же опроса, обидчиками в половине случаев являлись одноклассники жертвы, а в трети — незнакомые подростки.

Примеры

Тайлер Клементи (2010)

Сосед 18-летнего Тайлера Клементи по студенческому общежитию Дарун Рави узнал о нетрадиционной ориентации Тайлера. В какой-то момент Тайлер попросил своего соседа освободить помещение для личной встречи. Дарун оставил в комнате ноутбук с возможностью дистанционного подключения к веб-камере.

Просматривая трансляцию, Дарун не просто вторгся в жизнь Тайлера, но и начал рассказывать о его встрече с другим мужчиной в Твиттере. После этого произошел еще один инцидент, в ходе которого Дарун узнал о запланированном свидании и пригласил своих подписчиков в Твиттере подключиться к камере. Тайлер стал предметом насмешек в новой социальной среде. 22 сентября 2010 года Тайлер Клементи покончил с собой, спрыгнув с моста Джорджа Вашингтона.

Дарун Рави был приговорен к 30 дням заключения. Суд также назначил Даруну 3 года испытательного срока, 300 часов общественных работ и обязательное посещение консультаций по кибербуллингу. Помимо этого его оштрафовали на 10 000 долларов США.

Арсений Кураев (2021)

Выпускник Московской школы № 1297 Мещанского района, 18-летний подросток Арсений Кураев, был задержан правоохранительными органами за попытку совершения хулиганства с применением оружия. Данный поступок был вызван издевательством бывших одноклассников и учеников школы над Арсением. В число издевательств входили публикации его фотографий с оскорблениями в соцсетях, обсуждения Арсения в чатах и другое.

Очередной конфликт привел к тому, что сверстник выложил видео с унижением Арсения в соцсети. Тогда Арсений пообещал пристрелить своих обидчиков. Один из учеников школы сообщил об этой угрозе педагогу, что позволило предотвратить потенциальную трагедию.
9 декабря 2021 года Арсению Кураеву было предъявлено обвинение по статье о приготовлении к хулиганству с применением оружия. Ему грозит 7 лет лишения свободы.

Источники

1. «Арестован 18-летний москвич, угрожавший напасть на школу». Интерфакс (2021), https://www.interfax.ru/russia/808422
2. Bennett, D., et al. «College students' electronic victimization in friendships and dating relationships: Anticipated distress and associations with risky behaviors» (2011)
3. Chun, J., et al. «An international systematic review of cyberbullying measurements» (2020)
4. Englander, E., et al. «Defining Cyberbullying» (2017)
5. Hamm, M., et al. «Prevalence and Effect of Cyberbullying on Children and Young People» (2015)
6. Hinduja, S. and J. Patchin. «Summary of Our Cyberbullying Research (2007-2019)» (2019)
7. Mahanta, D. and S. Khatoniyar. «Cyberbullying and Its Impact on Mental Health of Adolescents» (2019)
8. Salin, D., et al. «Workplace bullying across the globe: a cross-cultural comparison» (2018)
9. Sourander, A., et al. «Psychosocial Risk Factors Associated With Cyberbullying Among Adolescents» (2010)
10. «Cyberbullying: A global advisor survey». Ipsos Public Affairs (2018)
11. «Cyberbullying». Pew Research Center (2007)
12. «Microsoft research on cyberbullying in various countries worldwide». Microsoft (2012)
13. «Percentage of U.S. middle and high school students who were cyber bullied as of April 2019, by type of bullying and gender». Statista (2021),https://www.statista.com/statistics/291034/cyber-bullying-share-of-us-students-by-type-and-gender/
14. «Roommate in Tyler Clementi Case Pleads Guilty to Attempted Invasion of Privacy». New York Times (2016), https://www.nytimes.com/2016/10/28/nyregion/dharun-ravi-tyler-clementi-case-guilty-plea.html

15. «Student Reports of Bullying: Results From the 2017 School Crime Supplement to the National Crime Victimization Survey». U.S. DEPARTMENT OF EDUCATION (2019)
16. «Teens and the Screen study: Exploring Online Privacy, Social Networking and Cyberbullying». McAfee (2014)
17. «What is cyberbullying and how to stop it». UNICEF

10. Сталкинг

Сталкинг — паттерн поведения, проявляющийся в навязчивом преследовании, выслеживании и продолжительных домогательствах до жертвы. Отличается высокой длительностью, пристальным вниманием к действиям жертвы.

Сталкер может использовать широкий спектр тактик и подходов в своих домогательствах и слежке за жертвой. Например, обычные и электронные письма, звонки, сообщения и другие действия в соцсетях, установка программного обеспечения для мониторинга на устройства жертвы.

Сталкинг вызывает у жертвы спектр негативных эмоций, главными из которых являются страх и ощущение потери контроля над жизнью.

Специфика риска

Помимо того, что сталкеры используют электронные письма, звонки, сообщения и другие действия в соцсетях, они могут организовывать встречи или общение с жертвой под видом другого человека или посредством людей из окружения жертвы, а также целенаправленно посещать места, в которых появляется жертва.

Существует отдельная категория программ, предназначенных или используемых для сталкинга, которая называется stalkerware. Известны кейсы, в которых сталкеры проявляли высокую степень изобретательности в отношении своего подхода к преследованию. Например, в случае с японской исполнительницей песен, сталкер нашел ее место жительства по отражению в ее зрачках на опубликованной фотографии.

В большинстве случаев сталкером является знакомый жертвы. Лидирующей категорией являются бывшие и нынешние партнеры, но сталкером также может оказаться коллега, одноклассник, сосед или незнакомец.

Дети-сталкеры чаще всего следят за своими сверстниками или людьми, которых они уже знают. Тенденция значительно меняется с возрастом — чем старше злоумышленник, тем выше вероятность того, что жертва является более молодой или бывшим партнером. Кроме того, подростки чаще меняют своих жертв.

Последствия сталкинга

У сталкинга есть длинный список последствий, большую часть из которых можно разделить на конкретные группы.

Ущерб здоровью: изменения веса, прямое и насильственное столкновение со сталкером, головные боли, усталость, проблемы со сном, слабость, тошнота.

Психологический ущерб: панические атаки, тревожность, ярость, недоверие, паранойя, агорафобия, посттравматическое стрессовое расстройство, страх за благосостояние своих близких, попытки суицида и мысли о суициде, причинении физического вреда себе.

Социальный, экономический ущерб и изменения в поведении: смена места жительства, работы или учебы, остановка социальных активностей и контактов, разрыв отношений с семьей и друзьями, смена имени и других легальных координат, смена телефонного номера и

электронной почты, смена аккаунтов в соцсетях, потеря денег, использование алкоголя и наркотиков.

Список не является исчерпывающим. Каждое из последствий может вызывать или повышать вероятность новых последствий или влиять на жертву одновременно в нескольких измерениях, например: потеря контакта с семьей может лишить жертву доли денежных средств или усилить интенсивность психологических последствий, а панические атаки могут мешать устанавливать и поддерживать социальные связи.

Постоянный страх и тревога жертв заставляют их идти на крайние меры и изменение своих привычек онлайн и офлайн. Жертвы, испытывающие более чем одну стратегию сталкинга, наиболее подвержены последствиям всех категорий — интенсивность, длительность и разнообразие подходов в плане домогательств повышают отрицательные эффекты преследования.

Подростковая проблематика в разрезе соцсетей

Около 45 % подростков ежедневно проводят в сети от 1 до 4 часов, а 39 % — более 4 часов в день. 69 % времени, которое дети проводят в интернете, уходит на соцсети.

В рамках использования социальных сетей дети регулярно проверяют профили своих друзей, знакомых, одноклассников и других лиц, которыми они интересуются. Обычной практикой является создание аккаунтов в нескольких соцсетях сразу, поэтому часто ребенок вынужден отслеживать обновления на множестве сайтов.

Поэтому кибersталкинг не сразу проявляется как нездоровое поведение или вовсе нормализуется политикой платформ и взглядами общества. Сами же дети встают таким образом на тонкую грань между сталкингом и здоровым интересом к своим близким и кумирам.

Распространенность

Согласно опросу в Великобритании, большинство респондентов считает, что кибersталкинг должен наказываться точно так же, как сталкинг. Можно сделать вывод, что общество не видит особой разницы между этими двумя преступлениями. 39 % опрошенных сочувствовали жертвам, а 35 % сказали, что жертвам нужно было разобраться в безопасном использовании интернета до того, как начать активно взаимодействовать с технологиями. 9 из 10 опрошенных были способны правильно определить психологические последствия сталкинга, а 8 из 10 — социальные. Лишь 34 % людей ответили, что у сталкинга есть психологические, социальные, физические и экономические последствия. 62 % опрошенных сказали, что нужно повышать осведомленность о кибersталкинге. 88 % согласились, что публикация личных данных в интернете является риском. 52 % опрошенных сказали, что они могут оказаться жертвой кибersталкинга, потому что жертвой может стать кто угодно.

Чаще всего жертвами сталкинга являются женщины, а сталкерами — мужчины. Но у женщин-сталкеров есть своя специфика: они чаще преследуют персон своего пола и чаще ищут и получают осознанную или неосознанную помощь от людей из окружения жертвы и своих собственных знакомых. По итогам исследования 2020 года, студентки являются жертвами сталкинга в 10 % случаев, а студенты — в 3 % случаев. По данным НКО SPARC, каждая 6-я женщина и каждый 17-й мужчина становятся жертвами сталкинга в течение своей жизни.

По результатам исследования 2009 года, объектом которого являлись ученики школ, 69 % жертв были девочками, причем ученицы старших и младших классов составили 71 % и 12 % соответственно от жертв женского пола из представленной в исследовании выборки. Получается, что закономерность о половом соотношении сохраняется между возрастами и остается статичной с течением времени.

Около 4 % сталкеров младше 16 лет, а 18 % злоумышленников — в возрасте от 16 до 19 лет. Доминирующая возрастная группа — люди в возрасте от 20 до 36 лет, —составляет 60 % от общего числа сталкеров.

Безработица, низкий самоконтроль и обсессивные расстройства личности коррелируют со злоумышленниками, которые занимаются сталкингом.

Среди взрослых, в контексте бывших и нынешних партнеров, самыми частыми формами кибersталкинга являются: проверка телефона (29 %); проверка истории браузера и поисковика (21 %); использование программ, которые позволяют следить за сообщениями, звонками, фотографиями и почтовой перепиской (10 %); создание ложных аккаунтов в соцсетях с целью проверки партнера (9 %); отслеживание физической активности партнера через приложения (8 %).

Статистика по стратегиям кибersталкинга, жертвам и сталкерам показывает, что существуют постоянные тенденции, которые могут меняться в зависимости от обстоятельств. Угрозы в интернете чаще всего направлены на мужчин, а все другие стратегии — на женщин.

Инфильтрация кругов общения жертвы и другие способы обмана с использованием чужой или сфабрикованной идентичности более свойственны незнакомцам, чем знакомым людям, хотя в других категориях лидируют знакомые жертве люди. Отсюда можно сделать вывод, что разные стратегии более или менее присущи разным категориям сталкеров и жертв.

Распределение мужчин и женщин в контексте разных практик сталкинга показывает, что пол играет роль в становлении жертвой и в том, какую тактику сталкинга будет использовать злоумышленник. Кроме того, в большинстве случаев сталкером является друг или знакомый.

Контакты онлайн: 28,4 % опрошенных ответили, что стали жертвами постоянных и навязчивых попыток установить контакт через интернет. Женщины составили 73,4 % жертв, мужчины были сталкерами в 73,5 % случаев. Сталкер был другом или знакомым в 53,8 % случаев и партнером или бывшим партнером в 20 % случаев, а на незнакомцев пришлось 26,2 %.

Домогательства в интернете: 19,3 % опрошенных ответили, что стали жертвами постоянных и навязчивых домогательств. Женщины составили 52,3 % жертв, мужчины были сталкерами в 67,6 % случаев. Сталкер был другом или знакомым в 60,4 % случаев и партнером или бывшим партнером в 16,3 % случаев, а на незнакомцев пришлось 23,3 %.

Сексуальные домогательства в интернете: 20,2 % опрошенных ответили, что стали жертвами сексуальных домогательств в контексте сталкинга. Женщины составили 73,9 % жертв, мужчины были сталкерами в 86,7 % случаев. Сталкер был другом или знакомым в 60,9 % случаев и партнером или бывшим партнером в 4,3 % случаев, а на незнакомцев пришлось 34,8 %.

Угрозы жертве в интернете: 11,8 % опрошенных ответили, что им угрожали в контексте сталкинга. Мужчины составили 53,8 % жертв, при этом они были сталкерами в 57,1 % случаев.

Сталкер был другом или знакомым в 66,7 % случаев и партнером или бывшим партнером в 11,1 % случаев, а на незнакомцев пришлось 22,2 %.

Использование сталкером идентичности других людей: 12,2 % опрошенных ответили, что стали жертвами сталкеров, которые воспользовались идентичностями других людей или сфабриковали новые. Женщины составили 53,6 % жертв, мужчины были сталкерами в 66,7 % случаев. Сталкер был другом или знакомым в 32,1 % случаев и партнером или бывшим партнером в 10,7 % случаев, а на незнакомцев пришлось 57,1 %.

Примеры

Барри Голдберг (2020)

57-летний Барри Голдберг был признан виновным в кибersталкинге, распространении и производстве детской порнографии в августе 2021.

Мужчина использовал схему сексуального вымогательства после того, как нашел релевантную информацию по своей жертве. Жертвой была 15-летняя жительница Сан-Франциско. Мужчина создал в соцсетях персоны мальчика-подростка, умирающего от рака, и его сестры. После этого он втерся в доверие к жертве и сумел получить от девочки контент сексуального характера. Он начал шантажировать жертву, угрожая опубликовать контент, если жертва не продолжит посылать ему новые фото и видео, снятые по его указаниям.

Барри регулярно преследовал жертву в интернете, отправлял ей сообщения сексуального характера и собирал информацию о ее окружении. Злоумышленнику удалось установить контакт и переписываться с некоторыми друзьями девочки под видом онлайн-персонажей. Барри не остановился на этом и присылал девочке сообщения, в которых говорил о том, что он владеет своей жертвой и не устанет ее эксплуатировать.

Расследование с участием ФБР позволило найти Барри Голдберга. По итогу обыска его дома было обнаружено, что он хранил контент порнографического характера на своем компьютере. По итогам суда Бари Голдберг получил 10 лет заключения и 10 лет испытательного срока после того, как заключение закончится.

Хибики Сато (2019)

Японского мужчину обвинили в сталкинге и сексуальных домогательствах после того, как он нашел место жительства японской певицы по отражению здания в ее зрачках на селфи. Из показаний преступника стало ясно, что он использовал Google Street View для того, чтобы определить, на какой станции метро живет его жертва. Он поджидал свою жертву на этой станции, потом последовал за ней до ее дома, а затем начал приставать к молодой исполнительнице. После ареста также выяснилось, что Хибики изучил все видео и фотографии, которые девушка сняла в своей квартире, узнав информацию вплоть до расположения штор и направления естественного света, чтобы определить местоположение квартиры.

Случай возродил общественную дискуссию о проблемах сталкинга и музыкальной индустрии в Японии. В 2018 году было известно о более чем 20 000 преступлениях, связанных со сталкингом в стране.

Источники

1. «Вместе за лучший Интернет: библиотеки, обслуживающие детей и их партнеры». Всероссийская видеоконференция (2019)
2. Acquadro Maran, Daniela, et al. «Health care professionals as victims of stalking: characteristics of the stalking behavior, consequences, and motivation in Italy» (2017)
3. Begotti, Tatiana and Daniela Acquadro Maran. «Characteristics of Cyberstalking Behavior, Consequences, and Coping Strategies: A Cross- Sectional Study in a Sample of Italian University Students» (2019)
4. Burlock, A. and T. Hudon. «Women and men who experienced cyberstalking in Canada». (2014)
5. Cantor, D., et al. «Report on the AAU campus climate survey on sexual assault and misconduct» (2020)
6. Dhir, A., et al. «The dark side of social media: Stalking, online self-disclosure and problematic sleep». (2021)
7. Malachiti, A. «Online Stalking and online activities An evaluation of risks and their perception». (2018)
8. Purcell, R., et al. «Stalking among juveniles» (2009)
9. Reyns, Bradford and Bonnie Fisher. «The Relationship Between Offline and Online Stalking Victimization: A Gender-Specific Analysis» (2018)
10. Sheridan, Lorraine, et al. «Stalking and age» (2014)
11. «Most common forms of cyber stalking an ex or current partner online according to adults in the United States as of December 2019». Statista (2021), https://www.statista.com/statistics/1189386/cyber-stalking-ex-current-partner-online/
12. «Number of reports of stalking in Italy in 2019, by gender of perpetrator». Statista (2021), https://www.statista.com/statistics/1077812/distribution-of-reports-of-stalking-by-gender-in-italy/
13. «Stalker 'found Japanese singer through reflection in her eyes». BBC (2019), https://www.bbc.com/news/world-asia-50000234
14. «Stalking Facts». Stalking Prevention, Awareness & Resource Center
15. «The State of Stalkerware in 2020». Kaspersky (2020)
16. «What is Stalking?» Stalking Prevention, Awareness, & Resource Center

11. Груминг

Груминг — это установление дружеского и эмоционального контакта с ребенком для его дальнейшей сексуальной или криминальной эксплуатации, мошенничества, шантажа, компрометирования или домогательств.

Онлайн-грумеры собирают информацию о детях и находят наиболее уязвимых жертв. Они знакомятся сразу с несколькими детьми, а затем выбирают свою жертву из тех, кто отреагировал на их сообщения, и анализируют соцсети ребенка, например, на предмет одиночества, нехватки внимания и заботы. После этого грумеры устанавливают психологический контакт с ребенком для дальнейшей реализации своих целей.

Специфика риска

Для корректного описания феномена следует различать офлайн- и онлайн-груминг.

Особенности офлайн-груминга

Офлайн-груминг требует тесной физической близости с детьми. Преступники могут скрываться на игровых площадках, детских спортивных мероприятиях или в других местах, ориентированных на молодежь, и многие из них часто берутся за работу в качестве специалистов по уходу за детьми или волонтеров, что обеспечивает им доверие и авторитет. В таких ситуациях преступник может выборочно дружить с уязвимыми детьми. Тем не менее, этот процесс требует личного риска для педофила, поскольку кто-то может заподозрить особое внимание или привязанность, направленные на ребенка.

Преступники полагаются на обман и манипуляции, чтобы избежать обнаружения и заручиться доверием ребенка и других взрослых. Педофилы умеют постепенно повышать интенсивность взаимодействия с ребенком, они осторожно манипулируют, чтобы ослабить его личные границы. В дополнение к вниманию и дружбе соблазнение может включать обмен подарками и специальные мероприятия или поездки. Педофил часто наживается на одиночестве или эмоциональной нужде ребенка. Как только преступник установит прочный контакт с ребенком, он может начать постепенно знакомить жертву с порнографией и впоследствии предлагать фотографировать ребенка в сексуализированных позах. Этот процесс предназначен для снижения чувствительности ребенка к наготе, стимуляции любопытства ребенка к сексу и подтверждения сексуальных отношений между взрослыми и детьми.

При столкновении с грумингом дети и подростки реагируют по-разному. Стивен Вэбстер предложил классифицировать жертв груминга как устойчивых, склонных к рискованному поведению и уязвимых.

Особенности онлайн-груминга

Из-за особенностей интернета киберпреступники одновременно имеют доступ к нескольким жертвам в среде. Педофилы также могут прятаться за защитным покровом анонимности, и даже притворяться детьми. Они могут изобразить любую личность или образ жизни, которые будут привлекательны для ребенка. Комнаты чатов, мессенджеры, электронные доски объявлений, адреса электронной почты и веб-сайты могут использоваться для привлечения потенциальных жертв и манипуляции ребенком, чтобы у преступника была возможность взаимодействовать с ребенком напрямую. Иллюзия приватности создает условия, в которых

молодежь будет общаться с незнакомыми людьми, что дает преступникам возможность подружиться и впоследствии обмануть ребенка.

Все преступления, относящиеся к онлайн-грумингу, имеют схожие признаки. Онлайн-грумеры обладают навыками сбора информации от детей, поиска профилей уязвимых целей и получения личной информации о конкретном ребенке.

Специфика и стратегии онлайн- и офлайн-груминга в целом похожи, но имеют и ряд отличий в манере и временном порядке их использования. Онлайн оценка риска и потенциала виктимизации встречаются чаще в начале коммуникации, а сексуальный контент — во второй половине взаимодействия с ребенком, однако переход к нему происходит значительно быстрее, чем офлайн.

Профиль злоумышленника

Не существует общего шаблона личности педофила. Чаще всего у людей с этим расстройством встречается:

1. чувство неполноценности;
2. изоляция от общества, одиночество;
3. низкая самооценка;
4. эмоциональная незрелость;
5. повышенный уровень пассивной агрессии и враждебности;
6. низкий уровень интеллекта;
7. иные различные психологические отклонения;
8. неосознанный выбор профессии (учитель в школе/университете, работа в детском саду и в детских секциях).

Человек, склонный к педофилии, не осознает этого и не испытывает чувства вины по отношению к жертве. По этой причине педофилы оправдывают свои действия и считают жертву согласной.

Выделяют 5 этапов поведения педофила в интернете:

1. знакомство, когда педофил пытается расположить к себе жертву;
2. формирование доверительных отношений, когда педофил демонстрирует свою честность и добросовестность;
3. оценка риска быть обнаруженным, когда педофил взвешивает вероятность склонности подростка к общению и к тому, что он поймет истинные цели педофила;
4. фаза эксклюзивных отношений, когда педофил обещает личные преимущества и услуги (деньги и ценные вещи);
5. сексуальная фаза, когда происходит первый физический контакт.

В том числе онлайн-педофилы могут преследовать разные цели:

1. вовлекать подростков в виртуальный секс (встреча в онлайне, создание детского порно), не требуя прямой встречи;
2. подталкивать и заставлять вступать детей в сексуальные отношения за пределами интернета.

Наибольшей уязвимостью отличаются подростки женского пола, неуверенные в себе и проверяющие собственную привлекательность (последнее касается и несовершеннолетних мужского пола). Имеют значение также низкая самооценка молодого человека, ограниченные

возможности здоровья, в том числе психического, социальная изоляция и слабая поддержка со стороны сверстников. В качестве защитных семейных факторов выступают родительский контроль за использованием ребенком интернета и знание ребенка об этом, а также позитивная поддержка ребенка со стороны родителей.

Распространенность

Исследование о киберпреступности, проведенное в Великобритании, показало, что в течение 2006 года в чатах было зарегистрировано 850 000 случаев нежелательных сексуальных переписок и 238 преступлений, связанных со встречей с ребенком после онлайн-груминга.

Исследование, проведенное в США в 2005 году, показало, что каждый 25 ребенок в возрасте 10-17 лет получал сообщения, содержащие сексуальные домогательства в агрессивной форме, которые включали попытки связаться с ним в автономном режиме. А один из 25 был привлечен грумером к тому, чтобы делать собственные фотографии сексуального характера.

Всего 5 лет спустя другое исследование показало, что каждый 11-й ребенок в США в возрасте от 10 до 17 лет сообщил о нежелательном сексуальном домогательстве в интернете.

Согласно статистике, 84 % официально зарегистрированных преступлений, относящихся к грумингу, связаны с девочками.

В 2012 году канадская служба CybertiPline установила 264 случая груминга среди детей 13-15 лет. В 93,4 % случаев были попытки получить детские фотографии сексуального характера. В 24 % случаев детям грозило распространение уже существующих изображений или другой вред. Потерпевшие отправляли свои фотографии педофилам в 30 % случаев. И в 35 % случаев преступники сами отправляли свои фотографии детям либо настаивали на взаимодействии с использованием видеосвязи.

Однако исследования, проведенные в промышленно развитых странах, показывают, что некоторые дети, ставшие жертвами онлайн-груминга, не имели очевидных негативных жизненных обстоятельств в прошлом и, по-видимому, были случайной мишенью. Этот факт демонстрирует, что типичной жертвы не существует, и самое поразительное в детях, подвергшихся насилию в интернете, это их неоднородность.

Некоторые грумеры общаются со многими детьми одновременно по мере развития их отношений. В 2012 году Европейский исследовательский проект онлайн-груминга обнаружил, что девочки подвергаются большему риску, чем мальчики. Так, мальчики составляют значительную группу жертв, но, как правило, менее охотно сообщают о случаях жестокого обращения.Таким образом, разрыв в подтвержденной виктимизации между мальчиками и девочками может быть меньше, чем указывается в некоторых сообщениях.

Министерством юстиции России было проведено исследование на основе 186 транскриптов диалогов между взрослыми людьми и несовершеннолетними, преимущественно они общались друг с другом в социальной сети «ВКонтакте».

Участниками диалогов стали 186 детей и подростков в возрасте от 8 до 17 лет (средний возраст — 13 лет), среди которых 15 мальчиков и 171 девочка, а также 13 мужчин в возрасте от 22 до 46 лет (средний возраст — 34 года).

Каждый из них совершил разное количество коммуникаций. Переписки осуществлялись с 2013 по 2017 год и имеют разные объемы (от 2 до более 1000 сообщений). Длительность диалогов варьируется от 1-2 дней до 3 месяцев, их средняя продолжительность составляет 5-7 дней.

Привлекшие внимание грумеров дети были разделены на 3 группы исходя из особенностей их общей реакции на новый контакт. 38,7 % от всех несовершеннолетних ответили отказом на предложение общения с взрослым независимо от предмета разговора. Чуть меньше детей — 26,3 % — были готовы общаться с взрослым, но исключительно на нейтральные темы. 4,9 % от общего числа детей были готовы разговаривать на темы сексуального характера, причем большинство вступало в диалог именно с взрослым человеком, а не с ребенком, за которого себя выдавал потенциальный грумер.

В большинстве случаев дети и подростки быстро отказывались от общения, несмотря на то, что в попытке завоевать доверие, грумеры начинали общение с нейтральных тем, делали комплименты или пытались их обмануть, выдавая себя за модельных агентов или режиссеров по кастингам, проявляли интерес к жизни, делам и увлечениям юных собеседников. Такие переписки, как правило, были краткосрочными.

Особенности реагирования детей данной группы можно условно поделить на общие реакции и способы прекратить общение.

К общим реакциям относятся: стремление получить информацию о грумере и его целях (15,4 %), о возрасте грумера (6,4 %); указание на отсутствие заинтересованности (12,9 %); отрицание наличия общих интересов с грумером (7,5 %); указание на свой юный возраст, возрастное несоответствие с грумером (5,9 %).

Второй тип реагирования сводился к прекращению переписки: вербальные агрессивные реакции, негативная оценка личности и поведения грумера (18,2 %); игнорирование сообщений грумера, повлекшее окончание переписки (7,5 %); вежливый отказ грумеру в продолжении общения (3,7 %); требование к грумеру прекратить присылать сообщения (3,7 %).

Примеры

Джастин Блоксом (2010)

Джастин Блоксом, двенадцатилетний мальчик, ночевал в доме своего друга. В тот день вечером он получил сообщение от девочки-подростка Эмбер. Джастин ответил, и Эмбер прислала фотографию сексуального характера. Пытаясь сменить тему разговора, Джастин отправил ей сообщение: «Ты должна помнить, что мне всего 12». Эмбер продолжала переписываться с Джастином до трех утра в течение четырех часов, пытаясь манипулировать Джастином и заставляя его поверить, что они должны встретиться лично. Вскоре после окончания переписки к дому подъехало такси, чтобы забрать Джастина.

В действительности «Эмбер» оказалась 34-летним таксистом Брайаном Хорном. Джастин Блоксом был найден 30 марта 2010 года задушенным и брошенным рядом с шоссе.

Кейли Хейвуд (2016)

В Великобритании с 15-летней Кейли Хейвуд связался 28-летний Люк Харлоу через Facebook*. В течение десятиминутной переписки они обменялись номерами мобильных телефонов, что стало отправной точкой для обмена более чем 2600 сообщениями. Две недели спустя Кейли

встретилась со своим грумером в его квартире, где ей дали значительное количество алкоголя, а затем изнасиловали и убили. Люк Харлоу и его сосед, 29-летний Стивен Бидман, соучастник преступления, были арестованы и заключены в тюрьму на 47 лет.

Этот случай, получивший значительное внимание средств массовой информации, вызвал озабоченность по поводу безопасности детей и подростков в интернете.

Адам Айзек (2016)

23-летний Адам Айзек из Уэльса использовал Minecraft, популярную видеоигру, чтобы поддерживать контакт за двумя мальчиками в возрасте 12 и 14 лет. Общение продолжалось по Скайпу, в мессенджерах и в Snapchat, поскольку разговоры становились все более сексуальным. Адам купил мальчикам подарки через PayPal, чтобы использовать их в игре и завоевать их доверие. В конечном счете он убедил их отправлять фотографии сексуального характера.

Адам Айзек был арестован в январе 2016 года и признал себя виновным в 8 сексуальных преступлениях против детей, что привело к приговору с наказанием в виде 2 лет и 8 месяцев тюремного заключения. Он также был пожизненно внесен в реестр сексуальных преступников.

Superfly1069 (2016)

В США с 14-летней девочкой под ником Superfly1069 связался через Instagram* другой пользователь, представившийся 16-летним мальчиком. За первым контактом последовали текстовые сообщения и развитие онлайн-отношений. Вскоре чаты стали более откровенными, когда мальчик стал отправлять сексуальные изображения и просить девушку сделать то же самое. Когда она отказалась, он пригрозил показать ее отцу откровенные чаты и изображения.

Выяснилось, что мальчик-подросток был отцом девочки, выдававшим себя за подростка. 41-летний мужчина признал себя виновным по 12 пунктам обвинения в склонении ребенка к производству детской порнографии, а также в получении и отправке детской порнографии. Он был приговорен к 20-летнему тюремному заключению и пожизненному надзору после освобождения.

Источники

1. Дозорцева Елена и Анна Медведева. «Сексуальный онлайн-груминг как объект психологического исследования» (2019)
2. Медведева Анна. «Реакции детей и подростков на сексуальный онлайн-груминг» (2020)
3. Babchishin, K., et al. «The characteristics of online sex offenders: a meta-analysis» (2011)
4. Berson, I.R. «Grooming cybervictims: The psychosocial effects of online exploitation for youth» (2003)
5. Black, P.J., et al. «A linguistic analysis of grooming strategies of online child sex offenders: implications for understanding of predatory sexual behavior in an increasingly computer-mediated world» (2015)
6. Egan, V., et al. «Sexual Offenders Against Children: The Influence of Personality and Obsessionality on Cognitive Distortions» (2005)
7. Hall, R. «A Profile of Pedophilia: Definition, Characteristics of Offenders, Recidivism, Treatment Outcomes, and Forensic Issues» (2007)
8. Jones, Lisa M., et al. «Trends in Youth Internet Victimization: Findings from Three Youth Internet Safety Surveys 2000-2010» (2011)

9. Maalla, Najat M'jid. «Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, including the Right to Development» (2009)
10. Mitchell, Kimberly, et al. «Trends in Youth Reports of Sexual Solicitations, Harassment and Unwanted Exposure to Pornography on the Internet» (2007)
11. Murray, J. «Psychological profile of pedophiles and child molesters» (2000)
12. O'Connell, R. «A typology of child cybersexploitation and online grooming practices» (2011)
13. Perrotta, G. «Pedophilia: Definition, classifications, criminological and neurobiological profiles, and clinical treatments. A complete review» (2020)
14. Perrotta, G. «Psicologia dinamica» (2019)
15. Webster, Stephen, et al. «European Online Grooming: Project final report» (2012)
16. Wolak, Janis, et al. «1 in 7 Youth: The Statistics about Online Sexual Solicitations» (2007)
17. «Child Safety Online: Global challenges and strategies». UNICEF. Technical Report (2012)
18. «Kayleigh Haywood: How murdered schoolgirl was groomed online». BBC News (2016), https://www.bbc.com/news/uk-england-leicestershire-36606210
19. «Kids interact at home with predators – via social media». Shreveport Times (2017), https://www.shreveporttimes.com/story/news/investigations/2017/05/25/kids-interact-predators-home-via-social-media/101801508/
20. «The man who posed as his daughter's online boyfriend to get nude photos of her». The Washington Post (2016), https://www.washingtonpost.com/news/true-crime/wp/2016/03/17/the-man-who-posed-as-his-daughters-online-boyfriend-to-get-nude-photos-of-her/
21. «Welsh gamer jailed for grooming two boys on Minecraft». The Guardian (2017), https://www.theguardian.com/uk-news/2017/jan/20/welsh-gamer-jailed-for-grooming-two-boys-on-minecraft

12. Сексуальные домогательства

Сексуальные домогательства включают в себя запугивание, издевательство или принуждение сексуального характера, а также нежелательное или ненадлежащее обещание вознаграждения в обмен на сексуальные услуги, иные устные или физические преследования сексуального характера.

К особенностям сексуальных домогательств в интернете также относят нежелательное половое поведение, выражаемое в использовании цифрового контента в частных переписках или на публичных платформах. Например, обмен изображениями и видео сексуального характера, принуждение и угрозы, издевательства на сексуальной почве.

У детей, которые становятся жертвами сексуального домогательства в интернете, проявляются серьезные отклонения в физическом и психологическом здоровье. Для каждой жертвы, подвергшейся домогательству, эти последствия уникальны. Домогательство в интернете может переходить в офлайн и принимать самую критическую форму — изнасилование.

Специфика риска

В российском законодательстве отсутствует определение «сексуального домогательства», наиболее близко к этому понятию подходит статья 133 Уголовного кодекса РФ — «Понуждение к действиям сексуального характера». Эта статья предусматривает уголовную ответственность за «понуждение лица к действию сексуального характера путем шантажа, угрозы уничтожением, повреждением или изъятием имущества либо с использованием зависимого положения потерпевшего/потерпевшей».

Можно выделить несколько категорий сексуальных домогательств в интернете. Они могут проходить параллельно, а также перекликаться с домогательством в офлайне:

1. обмен изображениями и видео интимного характера;
2. эксплуатация, принуждение и угрозы: получение угроз сексуального характера, принуждение к сексуальному поведению в интернете или шантажирование с использованием материалов с сексуальным подтекстом;
3. издевательства на сексуальной почве: группа людей, сообщество или отдельно взятый человек производят систематическое издевательство над человеком с использованием материалов сексуального характера, которые унижают, расстраивают или дискриминируют его;
4. нежелательная сексуализация (создание из человека сексуального образа): человек, получает нежелательные запросы, комментарии и материалы сексуального характера.

У жертв сексуального домогательства в интернете проявляются серьезные отклонения в физическом и психологическом здоровье.

Из-за пережитой травмы у жертв выявляются нарушение сна, расстройство питания, боли в животе, головные боли, сексуальные дисфункции. Это также может спровоцировать нанесение себе повреждений, а в крайних случаях — привести к суициду.

Влияние на эмоциональное состояние человека всегда индивидуально и может вызывать тревогу, депрессию, чувство вины, стыда. Все это чаще всего сказывается на успеваемости в учебе и на развитии человека как личности. Даже после восстановления проблемы

психологического характера могут возникнуть вновь из-за какого-либо подобного контента или события в жизни жертвы.

Для каждого лица, подвергшегося домогательству, эти последствия уникальны, а восстановление может длиться всю жизнь. Также домогательство в интернете может переходить в офлайн и принимать самую критическую форму — изнасилование. Ввиду этого, стоит внимательнее относиться к вопросу онлайн-домогательств и понимать потенциальный риск его развития и переход в офлайн.

Распространенность

В американском исследовании было выявлено, что 15 % подростков в возрасте 10-18 лет стали жертвами сексуального домогательства в интернете.

Чилийское исследование 2021 года показало, что 16,2 % детей 12-17 лет сталкивались с сексуальным домогательством онлайн хотя бы раз в своей жизни, причем девочки чаще становились жертвами (24,7 %), чем мальчики (8,8 %).

В том же исследовании было установлено, что сексуальное домогательство по отношению к девочкам чаще совершали взрослые мужчины (26,6 %) и мальчики до 18 лет (45,5 %). В свою очередь сексульное домогательство по отношению к мальчикам чаще совершали мальчики до 18 лет (14,8 %) и девочки до 18 лет (50,5 %).

Согласно европейскому исследованию 2017 года, проводившемуся в Великобритании, Дании и Венгрии, 10 % несовершеннолетних в возрасте от 13-17 лет получили угрозы сексуального характера в интернете от их сверстников в течение года.

Из исследования 2020 года, проведенного в Швеции, стало известно, что сексуальному домогательству в онлайне или в офлайне было подвержено 48,5 % девочек и 28,19 % мальчиков.

Из-за домогательств в интернете пострадало 24,41 % подростков в возрасте от 12-20 лет, преимущественно девушек — 26,7 %, тогда как мальчиков пострадало 20,7 %.

Жертвы сексуального насилия в подростковом возрасте в 4 раза более склонны к употреблению наркотических средств и алкоголя. Детская психика в 3 раза больше подвержена серьезным последствиям от сексуального домогательства и насилия, чем у взрослых.

По мнению более половины (55 %) детей, публикация обнаженных или интимных фотографий в интернете происходит по вине самой жертвы. При этом 22 % опрошенных детей считает, что получение комментариев сексуального характера в интернете — неизбежность, и они воспринимают это как норму.

В ходе исследования, проведенного в Швеции в 2020 году, выяснилось, что 44 % детей могли бы использовать сексуальное домогательство в интернете, чтобы навредить своим бывшим партнерам.

Отношение родителей

Согласно Малазийскому исследованию 2019 года, 95 % родителей знают о том, что дети подвергаются сексуальному домогательству во всем мире. При этом все 100 % респондентов считают, что домогательствами чаще всего занимаются мужчины.

Результаты исследования показывают, что большинство (80 %) родителей учат своих детей быть осторожными и аккуратными при общении с незнакомцами, а 74 % дают наставление своим детям отказывать, когда кто-то хочет к ним прикоснуться.

Примеры

Курьер из Delivery Club (2020)

В Подмосковье 11-летняя девочка подверглась домогательствам со стороны курьера Delivery Club, который привез еду из Burger King. Получив пакет с едой, девочка попрощалась с ним и ушла домой. Спустя пару часов он написал ей в WhatsApp. Она ответила, потому что сначала не поняла кто это. Курьер отправил ей сообщения сексуального характера, тогда девочка сообщила, сколько ей лет. На это она получила ответ: «Я знаю, что ты маленькая». Девочка ответила ему отказом, и мужчина стер их переписку в соцсети. После инцидента курьер еще несколько раз пытался позвонить девочке, в один из разов на звонок ответил ее отец. После этого звонки прекратились.

Впоследствии номера клиентов были скрыты для курьеров в приложении Delivery Club, чтобы избежать подобных ситуаций в будущем.

Александр Мельников (2014)

21-летний москвич Александр Мельников познакомился с десятилетней девочкой из Казани в интернете. Он отправлял девочке порнографический контент (фото, видео, текст) и оказывал на нее сильное психологическое давление через угрозы. Так мужчина хотел подтолкнуть несовершеннолетнюю девочку к сексуальному контакту и созданию для него детской порнографии со своим участием.

Александр получил 6 лет лишения свободы. Этот случай с насилием в интернете стал первым в истории российской судебной практики и послужил толчком в развитии по данному вопросу.

Источники

1. Антошкина Наталия. «За домогательство в Сети — 6 лет тюрьмы. О первом приговоре интернет-маньяку». Radiovesti.ru, (2014), radiovesti.ru/brand/61178/episode/1413516.
2. Родионов, Валентина. «Курьер из Burger King домогался ребенка, пока родителей не было дома». Ридус, (2020), www.ridus.ru/news/336390.
3. «В Подмосковье курьер ресторана приставал к 11-летней девочке». Vesti.ru (2020), www.vesti.ru/article/2456881
4. Ahmad, A., et al. «Parental Sensitivity and Their Awareness on a Child Sexual Harassment» (2019)
5. Buchanan, N. and A. Mahoney. «Development of a scale measuring online sexual harassment: Examining gender differences and the emotional impact of sexual harassment victimization online» (2021)
6. Copp, J., et al. «Online sexual harassment and cyberbullying in a nationally representative sample of teens: Prevalence, predictors, and consequences» (2021)
7. Guerra, C., et al. «Online sexual harassment and depression in Chilean adolescents: Variations based on gender and age of the offenders» (2021)

8. Pina, A., et al. «An overview of the literature on sexual harassment: Perpetrator, theory, and treatment issues» (2009)
9. Stahl, S. and I. Dennhag. «Online and offline sexual harassment associations of anxiety and depression in an adolescent sample» (2020)
10. Thacker, R. and S. Gohmann. «Emotional and Psychological Consequences of Sexual Harassment: A Descriptive Study» (1996)
11. Zinzow, H., et al. «Prevalence and risk of psychiatric disorders as a function of variant rape histories: results from a national survey of women» (2012)
12. «First World Report on Violence and Health». World Health Organization (2002)
13. «Young people's experiences of online sexual harassment». Project «dsSHAME» report (2017)

Группа 4. Цифровая эксплуатация, использование ребенка для создания цифрового контента

К этой группе относятся риски, которые напрямую связаны с эксплуатацией ребенка или информации о нем в интернете, например: доксинг, создание и распространение материалов с детской порнографией, кража, сбор и эксплуатация персональных данных, а также шерентинг.

Так, персональные данные ребенка могут быть раскрыты и/или использованы неправомерно, что повлечет за собой угрозы его физическому, психоэмоциональному или финансовому благополучию. При этом ребенка могут использовать для создания цифрового контента самыми разными способами — от фотографий в блоге родителей, до незаконной эксплуатации детей в материалах сексуального характера.

13. Доксинг

Доксинг — публичное раскрытие в сети персональной информации о человеке или группе людей. К такой информации может относиться, например, настоящее имя, адрес проживания, места работы, данные родственников, номера телефонов, финансовая, медицинская и другая идентифицирующая информация.

Иногда под доксингом подразумевается не только публикация данных, но и процесс подготовки — сбор информации о жертве и близких жертвы посредством использования соцсетей, государственных отчетов, поисковиков и других источников информации.

Личная информация ребенка публикуется и распространяется без его согласия. Доксинг обычно производится намеренно, с целью отомстить, запугать, шантажировать или иным образом навредить жертве.

Специфика риска

Сам термин происходит от английского выражения «drop docs» (скинуть документы). Публикация личной информации существовала задолго до интернета, но термин появился в 90-х в среде хакеров. Конкурирующие группировки и личности ссорились и в некоторых случаях принимали решение обнародовать личную информацию оппонентов.

Одна из признанных в научном сообществе классификаций доксинга делит его по двум измерениям: цели злоумышленника и мотивации злоумышленника. У доксинга также есть несколько подвидов, которые обладают своей собственной спецификой и не до конца вписываются в рамки, описанные в данных типологиях.

Цели злоумышленника

Типология по целям разработана Дэвидом Дугласом, доктором Университета Квинсленда. Он профессионально исследует вопросы компьютерной этики и ответственных инноваций, а также взаимодействия общества и технологий. Целью злоумышленника в этом подходе является нанесение ущерба анонимности, неизвестности или репутации жертвы. В своих работах Дуглас выделяет следующие виды доксинга.

Деанонимизирующий доксинг: подразумевает собой сбор и публикацию личной информации с целью нарушения анонимности жертвы. Потеря анонимности может мешать экономическим, личным, академическим и профессиональным стремлениям личности, так как анонимность дает людям определенную защиту и свободу действий. К такому виду доксинга может относиться публикация настоящего имени, телефона, почты.

Нацеливающий доксинг: вид доксинга, который похож на предыдущий, но отличается тем, что при нем происходит публикация точных данных о физическом местонахождении человека — адреса или места проживания. Чаще всего этот вид представляет собой следующий этап после деанонимизации жертвы. Его отличие заключается в том, что он упрощает физический контакт с жертвой, переводит конфликт в реальную жизнь.

Хорошим примером здесь может послужить ситуация с медиаперсонами: имена музыкантов, журналистов, писателей, режиссеров и киноактеров известны и легко доступны в отличие от их адресов и места пребывания.

Делегитимизирующий доксинг: является публикацией конфиденциальных или ранее неизвестных данных с целью нанесения ущерба репутации и авторитету личности. В своей работе Дуглас приводит следующий пример: «Публикация информации о том, что девушка-подросток ищет услуги по аборту, является делегитимизирующим доксингом, так как ставит репутацию и благосостояние жертвы под риск». Вероятность того, что любой человек из окружения жертвы знает постыдные факты, приводит к тревожности, эмоциональным проблемам и проблемам в отношениях.

Мотивация злоумышленника

Метаанализ, опубликованный учеными в 2021 году, делит доксинг по мотивации злоумышленника. Среди них выделяется доксинг ради вымогательства, для удаления оппонента из среды, возмездия, получения контроля над человеком, построения собственной репутации злоумышленника, непреднамеренный доксинг и доксинг в общественных интересах, реальных или мнимых. При этом мотивации не являются взаимоисключающими.

Распространенность

В опросе о негативном опыте использования интернета 12 % респондентов включили доксинг в список угроз, с которыми они сталкивались.

Результаты подробного анализа файлов с интернет-ресурсов, сообщества которых занимаются доксингом, показали, что минимальный возраст жертв доксинга составил 10 лет, а средний — 21 год. 82 % жертв были мужского пола, а 16 % женского. Это значительно отличается от статистики большинства форм кибербуллинга, в которых жертвы женского пола встречаются чаще.

По содержанию в файлах встречалась конфиденциальная информация следующих видов:

- адрес — 90,1 %;
- телефонный номер — 61,2 %;
- адреса электронной почты — 53,7 %;
- информация о семье — 50,6 %;
- почтовый индекс — 48,9 %;
- IP-адрес — 40,3 %;
- никнеймы — 40,1 %;

– дата рождения — 33,4 %;
– интернет-провайдер — 21,6 %;
– финансовая информация — 15,7 %;
– школа — 10,3 %;
– пароли — 8,6 %.

Исследователи также отметили, что самая частая категория жертв была активными игроками в видеоигры.

Примеры

Эшли Мэдисон (2015)

Эшли Мэдисон (Ashley Madison) — канадский сервис знакомств, названный в честь его основателя. Особенностью сервиса является его позиционирование — он создан для людей, которые уже имеют постоянные отношения, но хотят найти партнера на стороне.

В 2015 году хакеры из группировки The Impact Team взломали сайт. Сначала они попытались шантажировать организацию под предлогом публикации полученных данных. Хакеры требовали закрытия сервиса в обмен на сохранение конфиденциальности собранных ими персональных данных 37 млн пользователей. Руководство сервиса не приняло требований группировки. Тогда преступники опубликовали первый список клиентов сервиса объемом в 10 гигабайт.

Потом хакеры выложили в открытый доступ архивы, содержавшие имена, сексуальные фантазии, данные кредитных карт и даже адреса пользователей, а также внутренние переписки руководства сервиса и другую конфиденциальную информацию. Кроме того, в компании Эшли Мэдисон предоставляли платные услуги по удалению информации своих клиентов со своих серверов. По результатам деятельности The Impact Team оказалось, что компания не удаляла информацию о клиентах.

Степень репутационного и психологического ущерба не поддается оценке, но известно как минимум о двух суицидах. Когда человек узнает, что ему изменяли, это имеет крайне негативные последствия для обоих партнеров и их детей.

Кейс Эшли Мэдисон привлекает внимание не только масштабом, но и тем, что данные о личных внебрачных отношениях партнеров были преданы широкой огласке. В базах данных содержались адреса и контактные данные, а некоторые пользователи получали письма, в которых их пытались шантажировать. В этих письмах были угрозы направить информацию родственникам потерпевших. За молчание хакеры требовали платить в биткоинах — 225 долларов на момент скандала.

Норвежский аналитик Пер Торнстейн в сфере кибербезопасности заявил, что среди аккаунтов было много ненастоящих или созданных в качестве злой шутки аккаунтов людей, которые регистрировались на сайте, но не доводили дело до встреч с потенциальными партнерами. На момент взлома на сайте не было процедуры для проверки почты пользователей и систем верификации, препятствующих созданию аккаунта на имя другого человека.

Из-за группового иска клиентов, материнская компания Эшли Мэдисон выплатила 11 млн долларов.

Взрыв на Бостонском марафоне (2013)

Во время розыска виновников взрыва на Бостонском марафоне пользователи социальной сети Reddit решили помочь правительству. Тысячи посетителей сайта начали искать информацию о злоумышленниках, изучая все доступные им источники. Но в ходе их расследования произошло множество ошибок. Модераторы раздела сайта не справлялись с координацией пользователей. В итоге пользователи решили, что террористом был Сунил Трипати — студент Брауновского института, родившийся в семье индийских иммигрантов и попавший на фото марафона. Сунил страдал от депрессии и пропал за месяц до теракта, а его родители создали страницы в соцсетях, чтобы люди помогли с ним связаться.

Когда пользователи Reddit решили, что Сунил — террорист, его родителям посыпались гневные сообщения, а его персональная информация была опубликована в интернете. Не только сын семьи Трипати оказался в центре внимания реддиторов — персональная информация о нескольких других людях была так же опубликована, потому что пользователи подумали, что те являются подозреваемыми. В их числе был 17-летний Салах Бахрум. Когда его данные были опубликованы, он решил приехать в отдел полиции и дать показания касательно своей невиновности.

Тело Сунила Трипати было найдено 23 апреля 2013 года, причиной смерти установили самоубийство. Действия пользователей Reddit не только навредили человеку и его семье: с большой вероятностью они помешали работе ФБР – публикация его данных сместила фокус внимания общественности с Тамерлана и Джохара Царнаевых, реальных преступников, на невинного человека, усложнив идентификацию злоумышленников.

Источники

1. Anderson, B. and M. A. Wood. «Doxxing: A Scoping Review and Typology».
2. Cano, A. and K. D. O'Leary. «Infidelity and separations precipitate major depressive episodes and symptoms of nonspecific depression and anxiety» (2000)
3. Douglas, David M. «Doxing: a conceptual analysis» (2016)
4. Marx, G.T. «What’s in a name? Some reflections on the sociology of anonymity» (1999)
5. Nussbaum, M. C. «Objectification and internet misogyny» (2010)
6. Rosie Shrout, M. and Daniel J. Weigel. «Infidelity’s aftermath: Appraisals, mental health, and health-compromising behaviors following a partner’s infidelity» (2017)
7. Snyder, P., et al. «Internet Measurement Conference». (2017)
8. The Office of the Privacy Commissioner for Personal Data
9. «Ashley Madison condemns attack as experts say hacked database is real». The Guardian (2015), https://www.theguardian.com/technology/2015/aug/19/ashley-madisons-hacked-customer-files-posted-online-as-threatened-say-reports
10. «Ashley Madison hacked, users threatened with exposure». CBS News (2015), https://www.cbsnews.com/news/ashley-madison-hacked-users-threatened-with-exposure/
11. «Ashley Madison parent in $11.2 million settlement over data breach». Reuters (2015), https://www.reuters.com/article/us-ashleymadison-settlement-idUSKBN19Z2F0
12. «Ashley Madison users now facing extortion». CNN Business (2015), https://money.cnn.com/2015/08/21/technology/ashley-madison-users-extorted/
13. «Ashley Madison: Suicides over website hack». BBC (2015), https://www.bbc.com/news/technology-34044506
14. «Body of Missing Student at Brown Is Discovered». New York Times (2013), https://edition.cnn.com/2013/04/25/us/rhode-island-missing-brown-student/index.html

15. «Boston bombing: How internet detectives got it very wrong». BBC (2013), https://www.bbc.com/news/technology-22214511
16. «Don’t judge Ashley Madison users too quickly, their accounts may be fake». Per Tornstein (2015)
17. «Hackers expose first Ashley Madison users». CBS News (2015), https://www.cbsnews.com/news/hackers-expose-first-ashley-madison-users/
18. «Hackers Finally Post Stolen Ashley Madison Data». WIRED (2015), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/
19. «How Reddit Fueled the Scanner-Happy Media to Out Innocent Boston 'Suspects'». The Atlantic (2013), https://www.theatlantic.com/technology/archive/2013/04/reddit-police-scanner-innocent-boston-suspects/316101/
20. «How to prevent online harassment from doxxing». U.S. Department of Homeland Security
21. «Most common negative online experiences according to global internet users as of June 2016». Statista (2016), https://www.statista.com/statistics/675947/negative-online-experiences/
22. «News Conference Re: Ashley Madison Website Hack». Police of Toronto (2015)
23. «The Teenager Pictured On New York Post Front Page Goes To Police To Clear Name». Business Insider (2013)

14. Создание и распространение материалов с детской порнографией

С развитием технологий порнографические материалы о детях в больших количествах создаются и передаются преступниками по всему миру.

Невозможно определить, сколько людей потребляет детскую порнографию, точно так же, как невозможно точно определить, сколько детей становятся жертвами детской порнографии.

Последствия для детей, ставших жертвами, крайне серьезны. Такие преступления напрямую связаны с насилием над детьми. А тот факт, что жестокое обращение было записано и распространено, усугубляет ситуацию.

Специфика риска

Единого для всех стран мира юридического определения детской порнографии не существует. В факультативном протоколе ООН к Конвенции о правах ребенка, касающемся торговли детьми, детской проституции и детской порнографии, последняя определяется как «любое изображение ребенка, участвующего в реальных или имитируемых явных сексуальных действиях, или любое изображение половых органов ребенка в основном в сексуальных целях».

Детская порнография сегодня рассматривается во многих странах как особо тяжкое преступление, совершая которое, злоумышленник использует уязвимость детей. Преступления, связанные с детской порнографией, определяются как посягательство не только на конкретного ребенка, использованного в материале, но и на детей в целом, поскольку детская порнография способствует сексуализации всех детей.

Известно, что это отлично финансируемый бизнес, который постоянно растет благодаря технологическим достижениям. Развитие и возможности интернета только способствуют усугублению ситуации, поскольку изображения и видео, опубликованные в интернете, практически невозможно полностью удалить. Интернет обострил проблему детской порнографии за счет увеличения объема доступных материалов, эффективности их распространения и доступности. Интернет дает доступ к огромному количеству порнографических изображений со всего мира и делает порнографию доступной в любое время и в любом месте. Он позволяет получать доступ к контенту анонимно и конфиденциально, облегчает прямое общение и обмен изображениями между пользователями, позволяет дешевле распространять порнографию и обеспечивает изображения высокого цифрового качества.

Дети, ставшие жертвами таких преступлений, могут страдать от последствий в течение долгих лет. У них часто развивается депрессия и чувство вины. Кроме того, преступления, связанные с детской порнографией, напрямую связаны с насилием над детьми. Помимо того, что некоторые детские порнографические материалы изображают физическое сексуальное насилие над детьми, тот факт, что жестокое обращение было записано, распространено и просмотрено, усугубляет виктимизацию и жестокое обращение с жертвами. Травма усиливается из-за знания о том, что записанное и изображенное насилие распространяется и доставляет удовольствие другим.

Распространенность

В интернете можно найти более 1 млн порнографических изображений детей, причем ежедневно публикуется в среднем 200 новых изображений, считают исследователи. Сообщалось, что один из сайтов с детской порнографией получил 1 млн просмотров за месяц. Одна из проблем при оценке количества сайтов заключается в том, что многие из них существуют лишь в течение короткого периода времени, прежде чем их закрывают, и большая часть торговли детской порнографией происходит на скрытых уровнях интернета.

По оценкам, в организованных порнографических кругах по всему миру насчитывается от 50 000 до 100 000 педофилов, и треть из них работает в США.

При опросе выяснилось, что только 5 из 100 жертв злоумышленников обратились за помощью к правоохранительным органам. Интервью показали, что дети и подростки испытывали страх и стыд, а в некоторых случаях преступникам удавалось добиться лояльности ребенка.

Жертвами преступлений, связанных с детской порнографией, становятся дети всех возрастов, начиная от младенцев и заканчивая подростками. Лица, совершающие эти преступления — обычно мужчины, принадлежащие к широкому кругу социально-экономических групп.

В период с 2010 по 2020 год количество сообщений о распространения детской порнографии выросло до 750 тысяч. Также за 2019 год было выявлено свыше 3 млн фотографий и видеозаписей, содержащих материалы детской порнографии.

Не существует определенного типа пользователей детской порнографии в интернете, и нет простого и универсального способа распознать преступника. Наличие предвзятого представления о сексуальном преступнике-ребенке может оказаться бесполезным и отвлечь внимание полиции, проводящей расследование.

Примеры

Тренер из Твери (2022)

Тренера спортивной школы из Твери приговорили к 5 годам заключения. Он обвинялся более чем в 25 эпизодах за хранение и сбыт детской порнографии. Тренер распространял через интернет порнографические изображения детей, не достигших 14 лет. 4 февраля 2022 года он был признан виновным.

Джейсон Пол Уайт (2022)

Джейсон Пол Уайт — мужчина из Лаббока, штат Техас, который признал себя виновным в производстве детской порнографии в сентябре 2021 года. Согласно судебным документам, в 2009 году, когда Джейсону было 29 лет, он убедил ребенка заняться сексом для создания видео. Джейсон также выпустил 6 порнографических видео с тем же ребенком. В рамках признания своей вины Джейсон Уайт рассказал, что соблазнил 6 других несовершеннолетних мальчиков в период с 2004 года по 2020 год. Преступник был приговорен к 30 годам тюремного заключения с пожизненным надзором после освобождения. В рамках приговора обвиняемый также был обязан выплатить более 58 000 долларов США в качестве моральной компенсации жертвам.

Dreamboard (2013)

Dreamboard — онлайн-доска объявлений, созданная для организации и поощрения сексуального насилия над детьми.

Согласно судебным документам, участники Dreamboard обменивались изображениями и видео детской порнографии. Потенциальные желающие вступить в сообщество должны были создавать и делиться детской порнографией, чтобы получить членство в группе и поддерживать свой «статус участника». Члены Dreamboard предприняли различные технические и операционные меры, чтобы скрыть свою преступную деятельность от правоохранительных органов.

В результате операции Delego были предъявлены обвинения в общей сложности 72 преступникам. 57 из них были арестованы, 47 обвиняемых признали себя виновными в своей роли в заговоре, а еще один обвиняемый был осужден уже после основного судебного процесса.

Сергей Кропочкин (2011)

Сергей Кропочкин являлся основателем фотостудии «Сибирские мышки». У него обнаружили внушительный архив с изображениями обнаженных подростков. На протяжении 15 лет Сергей представлялся фотографом модельного агентства и заманивал девочек на съемки. Его признали виновным в совершении 145 эпизодов насильственных преступлений сексуального характера в отношении несовершеннолетних девочек. Материалы продавались в даркнете, а многих девушек травили в соцсетях.

Источники

1. Рыков Валерий. «Взаимодействие государств-участников ЕС в борьбе с сексуальной эксплуатацией детей и детской порнографией» (2021)
2. «В Твери тренера осудили на пять лет за детскую порнографию». Вести. Тверь (2022), https://vesti-tver.ru/dailynews/v-tveri-trenera-osudili-na-pyat-let-za-detskuyu-pornografiyu/
3. «Новосибирский фотограф в конспиративной квартире снимал и насиловал школьниц — чтобы задержать преступника, понадобилась помощь Интерпола». NGS.ru (2014), https://ngs.ru/text/gorod/2014/02/19/1674228/
4. Directive 2011/92/EU of the European Parliament and of the council
5. Jenkins, P. «Beyond Tolerance: Child Pornography on the Internet». New York: New York University Press (2001)
6. Optional protocol to the Convention on the Rights of the child on the sale of children, child prostitution and child pornography
7. Simon, L. «An Examination of the Assumptions of Specialization, Mental Disorder, and Dangerousness in Sex Offenders». Behavioral Sciences and the Law (2000)
8. Stanley, Janet Robin. «Child Abuse and the Internet» (2001)
9. Sundquist, Joanna Sanchez. «The problem of child pornography». UMEA University (2020)
10. Taylor, Max and Ethel Quayle. «Child Pornography: An Internet Crime» (2003)
11. Wortley, Richard and Stephen Smallbone. «Child pornography on the Internet» Problem-Specific Guides Series. Problem-Oriented Guides for Police № 41 (2012)

12. «2 plead guilty in one of largest child pornography cases in US history». U.S. Immigration and Customs Enforcement (2013), https://www.ice.gov/news/releases/2-plead-guilty-one-largest-child-pornography-cases-us-history
13. «Harm being done to Australian children through access to pornography on the Internet». Church and nation committee
14. «Man Sentenced to 30 Years for Production of Child Pornography». The United States Department of Justice (2022), https://www.justice.gov/opa/pr/man-sentenced-30-years-production-child-pornography
15. «Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse». Interagency working group on sexual exploitation of children (2016)

15. Кража, сбор и эксплуатация персональных данных

Эксплуатация персональных данных подразумевает получение доступа к личным данным детей и сбор этой информации незаконным способом, а также без согласия самих детей и их родителей, включая дальнейшее неправомерное использование. Также к данному риску относятся данные, полученные законным путем, но использующиеся в корыстных целях.

Чаще всего дети сами указывают личную информацию в интернете и свободно делятся ею с другими людьми. При этом они считают конфиденциальной информацией только контактные данные и не испытывают беспокойства за фото- и видеоконтент, который публикуют.

Доступ к личным данным открывает возможности для других правонарушений и рисков, связанных с опасностью для психического и физического здоровья жертвы.

Специфика риска

Кража, сбор и эксплуатация персональных данных нарушают приватность. Если рассматривать приватность человека шире, чем просто целостность персональных данных, можно выделить 4 типа приватности:

1. физическая приватность личности — защита организма человека от нежелательных воздействий на него;
2. приватность поведения личности — сексуальные предпочтения и привычки, политические и религиозные взгляды, защита личного пространства и приватных мест от несанкционированных наблюдений и вторжений;
3. приватность персональных коммуникаций — право на свободу коммуникаций, тайну переписки, в том числе электронной, и телефонных переговоров, защита от слежки;
4. приватность персональной информации — обеспечение прав граждан в области персональных данных, включая их циркуляцию, защиту и контроль.

Доступ к персональным данным открывает возможности для других правонарушений и рисков, связанных с опасностью для психического и физического здоровья жертвы. Если рассматривать эксплуатацию персональных данных в рамках отдельных случаев, где эти данные были получены или использованы незаконным путем, то конечной целью преступника зачастую является более опасное правонарушение, чем сам факт обладания чувствительными данными.

С одной стороны, интернет предоставляет новые инструменты, которые позволяют детям исследовать мир вокруг них. С другой стороны, он открывает новые возможности для отслеживания, хранения и анализа данных о действиях детей с недостижимым ранее уровнем

детализации. Массовое онлайн-наблюдение затрагивает не только права на неприкосновенность частной жизни, но, например, право на свободу выражения мнений.

Дети могут стать жертвой неправомерной эксплуатации данных по причине того, что сами указывают личную информацию в интернете, а также делятся ей с другими людьми. Так, например, только по информации из социальной сети можно составить портрет ребенка и узнать его местонахождение, контактные данные, хронику личных событий, внешность, социальные связи, материально-экономическое положение, образ жизни и поведенческие установки.

Социальные сети отслеживают каждое действие пользователя. Например, Instagram* оставляет за собой право анализировать все, что попадает в кадр, если человек использует камеру в приложении. При этом подростки не воспринимают фотографии, сообщения, список друзей, личную информацию на странице в социальных сетях как персональные данные. Большинство из них задумываются о проблемах с персональными данными только тогда, когда речь идет о контактной информации.

Особую роль для отслеживания поведения пользователя в браузере играют cookie-файлы. Благодаря cookie сайт распознает и записывает цель посещения страницы, действия пользователя, продолжительность нахождения на сайте, а также проводит аутентификацию пользователя, хранит персональные предпочтения и настройки. Эта аккумулируемая информация позволяет создать профиль пользователя, что является потенциальной угрозой конфиденциальности.

Помимо этого, данные детей могут быть украдены злоумышленниками. Число обращений, связанных со столкновением с вредоносными программами, постепенно снижается, с освоением новых устройств и приложений — растет, а со взломом аккаунтов и кражей персональных данных — остается постоянным.

В отчете, подготовленном по заказу ЮНИСЕФ, подчеркивается, что онлайн-наблюдение может быть еще более опасным для детей, растущих сегодня, поскольку массовый сбор данных позволит создавать и поддерживать записи всего цифрового существования детей.

Источником информации для цифрового профиля может стать любая активность ребенка в интернете и социальных сетях: посты, блоги, лайки, фотографии, рисунки, онлайн-заказы. Каждое действие пользователя оставляет цифровой след, цифровой отпечаток. Информация, публикуемая ребенком в интернете, может повлечь за собой последствия, которые проявятся не сразу, а в долгосрочной перспективе.

Раскрытие личной информации ребенка может привести к неприемлемым контактам, сексуальной эксплуатации или похищению. Помимо физических рисков, злоумышленники могут использовать детскую информацию в различных финансовых махинациях и других преступлениях.

Распространенность

Неправомерное использование личных данных детей в отдельных странах Центральной и Восточной Европы с 2017 по 2019 год показало, что больше всего уязвимы подростки в возрасте 15-16 лет.

Javelin Strategy, компания из сферы безопасности, обнаружила, что в 2017 году более 1 млн детей стали жертвами кражи личной информации в США. В 2021 году каждый 50-й ребенок страдает от мошенничества с кражей личной информации, что ежегодно обходится американским семьям почти в 1 млрд долларов.

Каждый десятый российский школьник (11 %) за последний год называл CVC-код незнакомому человеку. При этом 14 % детей публиковали в интернете детали банковской карты, а 12 % — свои паспортные данные.

Кража персональных данных

Каждый четвертый ребенок (26 %) сталкивался в сети с обманом и кражей личных данных. При этом дети 13–14 лет чаще всего попадали в ситуацию, когда кто-то использовал личную информацию, предоставленную ребенком в интернете, для розыгрыша или оскорбления (14 %). Жертвами кражи пароля для тех же целей чаще становились дети 15-16 лет (21 %).

Конфиденциальность данных в приложениях

Исследование, проведенное в 2021 году, показало, что 20 % приложений для детей в Google Play нарушают правила конфиденциальности. 80 % приложений родительского контроля запрашивают доступ к местоположению, контактам и хранилищу. Хотя эти разрешения помогают приложениям осуществлять детальный мониторинг, некоторые из них могут оказаться необязательными для того, чтобы приложение функционировало. Например, несколько приложений, предназначенных для отслеживания онлайн-активности детей запрашивают такие разрешения, как «чтение календаря», «чтение контактов» и «запись аудио», причем это не указано ни в описании приложения, ни в политике конфиденциальности.

Примеры

Похищение Ивана Касперского (2011)

У сооснователя и руководителя «Лаборатории Касперского» Евгения Касперского в 2011 году похитили сына и требовали выкуп в размере 3 млн евро. В своем блоге Евгений Касперский написал, что преступники использовали открытые данные из социальных сетей, в том числе из социальной сети «ВКонтакте», где Иван указал «более чем достаточно деталей, чтобы понять распорядок его жизни, предпочтения и работу и спланировать преступление».

Сотрудники спецслужб освободили сына Евгения Касперского, а похитители были привлечены к ответственности.

Цифровой след абитуриента (2017)

Гарвардский колледж отказал в поступлении десяти потенциальным студентам после того, как они обменялись откровенными и жестокими картинками и сообщениями в групповом чате Facebook*. Абитуриенты присылали друг другу изображения, в которых насмехались над сексуальным насилием и смертью детей. В некоторых сообщениях они шутили, что их возбуждает жестокое обращение с детьми, а также высказывались против конкретных этнических или расовых групп.

Сами того не подозревая, потенциальные студенты Гарварда оставили в социальной сети цифровой след, который негативно повлиял на их поступление в колледж. Сотрудники колледжа заявили, что решение Гарварда отказать студентам в зачислении является окончательным.

Взлом Wildworks (2020)

Wildworks — компания, производящая мобильные и компьютерные игры для детей. В 2020 году хакеры получили доступ к облачной инфраструктуре компании из-за состоявшегося ранее взлома серверов мессенджера Slack.

В руках хакеров оказались персональные данные более 46 млн людей, которые включали имена, возраст, банковские данные, IP-адреса, половую принадлежность жертв — как родителей, так и детей. Преступление было выполнено группой ShinyHunters, причем вскоре после взлома были опубликованы две базы данных, суммарно содержавшие информацию о 7 млн человек. Публикацию совершил другой злоумышленник, который купил у группировки часть украденной информации.

Источники

1. Благовещенский Антон. «Евгений Касперский: Соцсети сыграли решающую роль в похищении сына». Российская газета (2011), rg.ru/2011/05/18/kasperskii-site-anons.html.
2. Богданова Диана.«Информационный мир: новые игрушки». Школьные технологии № 1 (2018)
3. Касперский Евгений. «Дети и соцсети. Проблема, которую лучше решить поздно, чем никогда». (2011), e-kaspersky.livejournal.com/64468.html.
4. Петров А.А. «Цифровой след человека: плюсы и минусы». Большая Евразия: Развитие, безопасность, сотрудничество 3-2 (2020): 529-542.
5. Политика использования данных Instagram, https://help.instagram.com/519522125107875
6. Смирнов Игорь. «Не надо разбрасываться своими персональными данными». Психология и педагогика служебной деятельности № 4 (2020)
7. Солдатова Г. У. и др. «Дети России онлайн: риски и безопасность. Результаты международного проекта EU Kids Online II в России» (2012)
8. Солдатова Г. У. и др. «Эволюция онлайн-рисков: итоги пятилетней работы линии помощи “Дети онлайн”». Консультативная психология и психотерапия 23.3 (2015): 50-66.
9. Солдатова Г. У. и Теславска О. И. «Отношение к приватности и защита персональных данных: вопросы безопасности российских детей и подростков». Национальный психологический журнал № 3 (19) (2015)
10. Солдатова Галина и Теславская О. И. «Персональные данные и дети: вопросы безопасности». Эпоха науки № 12 (2017)
11. «Каждый десятый школьник сообщал данные банковской карты незнакомцам». РИА Новости (2021), https://ria.ru/20210515/karty-1732410828.html
12. Gogus, Aytac and Yücel Saygın. «Privacy perception and information technology utilization of high school students». Heliyon № 5.5 (2019)
13. ICO PIA Handbook (2007)
14. Millman, Rene. «20 % of Google Play Apps Breach Child Privacy Rules». IT PRO (2021)
15. Pangrazio, Luci. «Apps That Help Parents Protect Kids from Cybercrime May Be Unsafe Too». The Conversation (2021)
16. «Animal Jam was hacked, and data stolen; here’s what parents need to know». TechCrunch (2020), https://techcrunch.com/2020/11/16/animal-jam-data-breach/
17. «Child Identity Fraud Study». Javelin Strategy (2018), https://www.javelinstrategy.com/coverage-area/2018-child-identity-fraud-study
18. «Child Identity Fraud: A Web of Deception and Loss». Javelin Strategy (2021), https://www.javelinstrategy.com/coverage-area/child-identity-theft-fraud
19. «Child Privacy in the Age of Web 2.0 and 3.0: Challenges and opportunities for policy». UNICEF (2017)
20. «Harvard Rescinds Acceptances for At Least Ten Students for Obscene Memes | News | The Harvard Crimson». The Harvard Crimson (2017), www.thecrimson.com/article/2017/6/5/2021-offers-rescinded-memes

21. «Personal data misuse experienced by children in the CEE region 2017-2019». Statista, https://www.statista.com/statistics/1190588/cee-personal-data-misuse-experienced-by-children-by-age/

16. Шерентинг

Шерентинг — это регулярное использование родителями социальных сетей для обмена новостями, изображениями и другой информацией о детях. Слово образовано от английских слов «share» — делиться, и «parenting» — воспитывать, растить ребенка.

Шерентинг может привести к искажению представлений о реальной жизни. Родители высказывают свою точку зрения, зачастую не спрашивая, что об этом думает сам ребенок. Публикуя посты о своих детях, родители сами создают цифровой портрет ребенка в интернете, тем самым вмешиваясь в его цифровую идентичность.

Помимо того, что родители публикуют фотографии своих детей и истории, связанные с их воспитанием, они также раскрывают конфиденциальную информацию о своих детях, которая может включать полное имя детей, дату рождения, вес, рост, геолокацию и другие данные.

Специфика риска

Выделяют четыре основные причины, по которым родители делятся личной жизнью своих детей в интернете: присутствие в сообществе, трансляция новых подходов, коммерциализация, социальное влияние.

1. Присутствие в сообществе. По результатам исследования 2019 года, в ходе которого проводилась серия интервью с матерями в возрасте от 24 до 40 лет, стало известно, что многие из них делились информацией о своих детях, чтобы справиться с проблемами и сложностями материнства. Аналогично и отец, занимающийся воспитанием ребенка, чувствует себя увиденным, услышанным и поддержанным сообществом других отцов. Шерентинг может быть вызван желанием получить поддержку от группы единомышленников, родителей с похожими подходами к воспитанию.

2. Трансляция новых подходов. Обмен мнениями и фотографиями в блоге позволяет родителям показать, что воспитание детей не всегда проходит идеально. Женщины, которые ведут блог о своих детях, делятся личными рассказами о стереотипах воспитания детей, навязанных обществом, расширяя тем самым понятие материнства.

3. Коммерциализация. Популярные в социальных сетях родители коммерциализируют свой блог благодаря рекламе. Несмотря на то, что изначально многие родители делятся информацией о своих детях по одной из двух вышеперечисленных причин, по мере развития блога они начинают извлекать из него и финансовую выгоду, заставляя детей делать то, что будет способствовать популярности аккаунта. Для некоторых родителей грань между получением дохода и производством контента ради первоначальной цели становится размытой.

4. Социальное влияние. Публикация семейной жизни в интернете вводит конкурентную составляющую в онлайн-взаимодействие с семьей, сверстниками и даже незнакомыми людьми. По результатам исследования 2016 года, в ходе которого опросили и проанализировали 168 родителей-блогеров из Польши, выяснилось, что существует положительная корреляция между количеством друзей родителей на Facebook* и количеством фотографий с их детьми. Кроме того, исследователи предположили, что шерентинг может быть формой «социального соревнования», в котором родители сравнивают свою повседневную жизнь, прогулки, события с жизнью других родителей. Шерентинг может вызвать у родителей эгоистичное желание

манипулировать другими, которое будет реализовываться благодаря неэтичному использованию контента с их детьми.

Последствия шерентинга

Родители несут ответственность и за себя, и за своих детей, когда публикуют фотографии и рассказывают о них в интернете, при этом шерентинг может укрепить потенциально вредные стереотипы. Например, подростки не должны чувствовать, что они обязаны носить определенную одежду или вести себя определенным образом, чтобы быть достойными публикации в Facebook* на страницах своих родителей.

Согласно британскому исследованию, дети от 8 до 12 лет зачастую испытывают неловкость и беспокойство, когда родители публикуют их фотографии. Они объясняли это тем, что не хотят, чтобы большая группа людей их видела, или детям не нравилось, как они выглядели на фотографии. Часть опрошенных детей выражала беспокойство по поводу того, что они никак не могут повлиять на публикацию фотографий их родителями.

Шерентинг может привести к искажению представлений о реальной жизни. Родители высказывают свою точку зрения, зачастую не спрашивая, что об этом думает сам ребенок. Публикуя посты о своих детях, родители сами создают цифровой портрет ребенка в интернете, тем самым вмешиваясь в его цифровую идентичность.

Распространенность

По результатам опроса, 32 % британских родителей в среднем загружают 11–20 новых фотографий ребенка каждый месяц. Более четверти (28 %) признались, что они никогда не задумывались о том, чтобы спросить у ребенка разрешения на публикацию фотографии в интернете. При том что большая часть (55 %) родителей никогда не задумывалась о возможных последствиях, только 6 % выразили беспокойство о возможном недовольстве ребенка опубликованными фотографиями. Также всего 9 % родителей задумывались о том, что фотографии смогут просматривать незнакомые люди.

50 % детей в возрасте от 12 до 14 лет выразили беспокойство по поводу того, что родители выкладывают фотографии с ними в социальные сети. Эта возрастная группа была выбрана потому, что молодые люди начинают исследовать свою личность в раннем подростковом возрасте. Но несмотря на то, что проблема особенно остро ощущается среди подростков, исследование, проведенное в США в 2010 году, обнаружило, что около 90 % детей приобретают цифровую идентичность уже в двухлетнем возрасте.

По прогнозам Barclays, к концу следующего десятилетия две трети случаев мошенничества с личными данными, с которыми сталкиваются дети и подростки, будут приходиться на шерентинг, при этом к 2030 году количество случаев хищения личных данных достигнет 7,4 млн.

Примеры

Конрад Итурбе (2019)

19-летний испанский программист Конрад Итурбе признается, что был крайне встревожен, когда в 14 лет узнал, что родители выкладывали его фотографии в социальные сети.

По словам молодого человека, у его мамы был аккаунт в Instagram* еще до того, как у него появился телефон, поэтому он даже не догадывался, что его фотографии могут быть где-то

размещены. Юноша не любит выкладывать фотографии в соцсети, а когда он увидел свои фото в профиле у мамы, то попросил удалить и уточнил, что не давал разрешения на публикацию.

Конрад воспринял такой поступок матери как вторжение в личное пространство. Особенно ему не понравилось, что там были фотографии его маленького, а профиль был открыт для всех. Его также беспокоит, что с помощью технологии распознавания лиц люди смогут отслеживать его и в более позднем возрасте.

DaddyOFive (2015-2019)

Популярный YouTube-канал DaddyOFive, который в 2015 году запустили молодые родители Майкл и Хизер Мартин, специализировался на видео-шалостях с участием пятерых детей. В видео на канале родители высмеивали свой собственный небрежный подход к воспитанию детей. На пике развития DaddyOFive имел около 750 тысяч подписчиков.
По мере развития канала выходки родителей становятся все более жестокими: видео включали в себя пощечины или крики на детей, родители говорили, что отдадут детей на усыновление, и ломали игрушки. Хотя Мартины утверждали, что это постановка, а их дети согласились играть свои роли, в ситуацию вмешались власти.

В ходе судебного разбирательства психолог обнаружил, что двое из детей, которым в то время было 9 и 11 лет, испытывали «наблюдаемые, идентифицируемые и существенные нарушения их умственных или психологических функций». Майкл и Хизер Мартин были приговорены к пяти годам условно, а видео были удалены. Адвокат семьи заверил суд, что пара станет более «осторожной» со своими детьми и социальными сетями.

Источники

1. Богданова Диана. «Sharenting — родительская любовь или безответственность?» Народное образование, № 1 (1472) (2019)
2. «Мам, не публикуй мои фотографии у себя в соцсетях!». Что такое «шерентинг?» BBC News Русская служба (2019), www.bbc.com/russian/features-47731823
3. Archer, Catherine. «How Influencer “Mumpreneur” Bloggers and “Everyday” Mums FramePresenting Their Children Online». Media International Australia, vol. 170, no. 1 (2019)
4. Blum-Ross, Alicia and Sonia Livingstone. ««Sharenting», parent blogging, and the boundaries of the digital self». Popular Communication 15.2 (2017): 110-125
5. Brosch, Anna. «When the Child Is Born into the Internet: Sharenting as a Growing Trend amongParents on Facebook». The New Educational Review, vol. 43, no. 1 (2016): 225–235
6. Campana, Mario, et al. «#dadtribe: Performing Sharenting Labour to Commercialise InvolvedFatherhood». Journal of Macromarketing, vol. 40, no. 4, (2020): 475–491
7. Coughlan, By Sean. «“Sharenting” Puts Young at Risk of Online Fraud». BBC News (2018), www.bbc.com/news/education-4415375
8. Fox, Alexa K. and Mariea Grubbs Hoy. «Smart Devices, Smart Decisions? Implications ofParents’ Sharenting for Children’s Online Privacy: An Investigation of Mothers». Journal of Public Policy & Marketing, vol. 38, no. 4, (2019): 414–432
9. Johannesen, Richard L, et al. «Ethics in Human Communication». Waveland Press (2008)
10. Lafrance, Adrienne. «The Perils of “Sharenting”». The Atlantic 6 (2016).
11. Lopez, Lori Kido. «The Radical Act of “Mommy Blogging”: Redefining Motherhood through the Blogosphere». New Media & Society, vol. 11, no. 5, (2009): 729–747
12. McTigue, Maddy. «Communication Ethics of «Sharenting»: A Content Analysis of Instagram Mom Meso-Influencers» (2021)

13. Ouvrein, Gaëlle and Karen Verswijvel. «Sharenting: Parental adoration or public humiliation? A focus group study on adolescents' experiences with sharenting against the background of their own impression management». Children and Youth Services Review 99 (2019): 319-327.
14. Rose, M. «The average parent shares almost 1,500 images of their child online before their 5th birthday». Parentzone (2018), https://parentzone.org.uk/article/average-parent-shares-almost-1500-images-their-child-online-their-5th-birthday
15. Sivak, Elizaveta and Ivan Smirnov. «Parents mention sons more often than daughters on social media». Proceedings of the National Academy of Sciences 116.6 (2019): 2039-2041
16. Song, Felicia Wu. «The Serious Business of Mommy Bloggers». Contexts, vol. 15, no. 3 (2016): 42–49
17. «Instagram, Facebook, and the Perils of “Sharenting”» The New Yorker (2019), www.newyorker.com/culture/cultural-comment/instagram-facebook-and-the-perils-of-sharenting
18. «Life in likes: Children’s Commissioner Report into social media use among 8–12 year olds». Children’s Commissioner (2018)

Группа 5. Информационное давление, информация, не предназначенная для детей и подростков

К этой группе относятся риски, в основе которых лежит информация, способная травмировать, дезинформировать, подтолкнуть ребенка к неверным выводам или опасным действиям, например: контент, содержащий сцены насилия, порнографический контент, дезинформация, а также опасные тренды и челленджи.

Контент, не предназначенный для детей и подростков, может негативно сказаться на их мировоззрении и привести к психологическим травмам, даже если изначально авторы контента не задавались такой целью.

17. Контент, содержащий сцены насилия

К такого рода контенту относится любая доступная для восприятия форма представления информации, воспроизводящая ситуации или действия насильственного характера, которые причиняют или могут причинить вред одному или нескольким лицам.

Дети учатся, наблюдая и пробуя поведенческие сценарии, поэтому они особенно восприимчивы к негативным последствиям, которые вызывает потребление контента с насилием.

Краткосрочные эффекты связаны с процессами возбуждения и непосредственной имитацией определенного поведения. Долгосрочные эффекты обусловлены более продолжительным изучением такого контента, из-за чего негативные эмоции детей по отношению к насилию постепенно уменьшаются, и формируются новые установки.

Специфика риска

Характеристика насилия весьма субъективна, и это создает трудности для однозначного определения контента с ним. В самом общем смысле насилие заключается в применении силы против кого-то с нанесением физических повреждений.

В современном мире практически каждый человек может создать контент, доступный большому количеству пользователей в интернете. Это ставит под удар детей и подростков, так как они более подвержены внешнему влиянию и манипуляциям. Такая ситуация создает необходимость в защите от нежелательной и вредоносной информации. Воздействие контента с насилием, как и наблюдение за насилием, происходящим в реальном мире, увеличивает риск насильственного поведения со стороны зрителя.

Выделяют факты, которые в любой культуре и социальной среде причисляются к насильственным — пытки, убийства, побои. Для других действий кросс-культурные критерии не одинаковы: насилие непосредственно внутри семьи против женщин и детей, тяжелые условия жизни в тюрьме во многих традиционных обществах долгое время считались и считаются нормой. Как пишет французский исследователь, профессор Ив Мишо, в обществе комфорта и прав, где правила поведения становятся все более регламентированы и стандартизированы, чувствительность к насилию может увеличиться. Это значит, что критерии, которые определяют социальный акт как насилие, становятся более широкими, и можем утверждать, что «насилие порождается в его представлении в том виде, в каком оно мыслится и конституируется как

социальный факт». Это наблюдение особенно важно в контексте данной работы, так как в нем затрагивается понятие мысли о насилии, а следовательно, и провоцирование соответствующих мыслей и последующего девиантного поведения после соприкосновения с контентом, содержащим насилие.

Последствия

Необходимо учитывать обеспокоенность общества по поводу подстрекательства к насилию путем распространения контента, который влияет на агрессивное поведение детей и подростков. Такой контент стимулирует импульсивную агрессию детей и провоцирует их агрессивное поведение в отдаленном будущем. Контент с насилием также формирует отношение к насилию как к норме поведения и способу разрешения проблемных ситуаций. Поэтому некоторые эффекты проявляются еще в детстве, а некоторые — уже в зрелом возрасте.

Согласно заключению Американской психологической ассоциации, навязываемые насильственные поведенческие сценарии и их повторяющееся воздействие посредством интернета имеют следующие последствия:

- усиление чувства враждебности и ожидания того, что другие будут вести себя агрессивно;
- снижение чувствительности к боли других и повышение вероятности применения насилия в социуме;
- негативное влияние на мыслительные способности и навязывание негативных или деструктивных моделей мышления и поведения.

В исследовании ученых МГУ имени М.В. Ломоносова отмечается также риск осложнения личностного развития ребенка и снижение уровня психологической безопасности. Это может привести к появлению тревожности, перепадам настроения, депрессии, неуверенности и страха за собственную безопасность и, как следствие, социальным фобиям и изоляции. Подобные последствия отмечают и другие исследователи. Все это может негативно отразиться на социальной и профессиональной жизни, а более тяжелые последствия включают совершение преступлений и покушение на свою жизнь.

Большинство теоретиков сходятся во мнении, что краткосрочные эффекты воздействия контента с насилием в основном связаны с процессами прайминга, возбуждения и непосредственной имитацией определенного поведения. Долгосрочные эффекты обусловлены более продолжительным наблюдением и изучением контента с насилием. Вследствие этого негативные эмоции детей по отношению к такому контенту постепенно уменьшаются.

Распространенность

По данным исследований российского Фонда развития интернета, проведенных в 2009 году, часть подростков осознает, что в интернете можно встретиться с контентом, содержащим насилие. Столкновение с такими материалами производит на подростков настолько сильное впечатление, что 76 % из опрошенных считают, что интернет опасен: 53 % из них заявляют об этом в категоричной форме, еще 23 % согласились с формулировкой «иногда опасен». У каждого десятого подростка интернет вызывает разочарование и гнев (11 %), и почти пятая часть (19 %) старшеклассников указали, что часто сталкиваются в интернете с информацией, которая раздражает их и вызывает неприятные эмоции.

По результатам опроса российских родителей, угроза контента с насилием в интернете стоит на третьем месте (9,9 %) после порнографического и эротического контента (14,9 %) и «групп смерти» в соцсетях (10,8 %). При этом 7% родителей считают, что интернет для их ребенка не представляет никакой угрозы.

В зависимости от возраста детей меняется и восприятие их родителями угроз в интернете. Для детей младше 7 лет основной угрозой (14,4 %) называют агрессию и жестокость, а порнографического и эротического контента и групп, склоняющих к суициду, больше всего боятся родители детей в возрасте 11-13 лет (по 16,3 %).

Среди мужчин, которые в детстве (7-12 лет) регулярно просматривали контент с насилием, 11 % имеют судимость за преступление, 42 % совершали насилие в семье, а 69 % проявляли агрессию по отношению к другим людей. Что касается женщин, то 39 % совершали насилие в семье, а 17 % проявляли агрессию. Отмечено, что эти показатели не были связаны ни с демографическими факторами, ни с интеллектом испытуемых, ни с методами их воспитания.

Примеры

Михаил Пивнев (2017)

Девятиклассник Михаил Пивнев открыл стрельбу в школе из пневматической винтовки, а затем взорвал самодельное взрывное устройство. По словам юноши, он решился на преступление после просмотра контента с действиями американских массовых убийц Эрика Харриса и Дилана Клиболда — преступников, атаковавших в апреле 1999 года колумбайнскую старшую школу.
Пострадали 4 человека: учительница, которой подросток нанес удар секачом по голове и выстрелил в лицо, а также трое учеников школы, выпрыгнувших из окна здания учебного заведения. Пивнев был приговорен к 7 годам и 3 месяцам лишения свободы с отбыванием наказания в воспитательной колонии.

Последователи «хабаровских живодерок» (2016)

Внимание двух девушек из Хабаровска в возрасте 12 и 13 лет привлекло видео с жестоким обращением с животными, авторами которого были Алина Орлова и Алена Савченко. Хабаровчанки решили воспроизвести увиденное, только без реальных мучений и убийств. Девушки выложили в сети фото, на которых они издеваются над котенком. Девочки измазали животное краской, похожей на кровь, сделали фотографии ножа рядом с ним, имитировали сцену, где они давят животное ногой, подражая известным фигуранткам уголовного дела.

Следственный комитет Хабаровского края провел проверку по сообщениям о подражательницах и официально опроверг, что над животным издевались по-настоящему. Фото и видео оказались инсценировкой. 13-летняя девочка сообщила, что выложила фотографии и видео в интернет с целью привлечения к себе внимания, которого ей не хватает в жизни.

Источники

1. Годик Ю. А. «Угрозы и риски безопасности детской и подростковой аудитории новых медиа» (2011)

2. Карабанова О. А. и С.В. Молчанов. Национальный психологический журнал № 3 (31) (2018)
3. Меренков Анатолий. «Родители и педагоги: растим ребенка вместе» (2005)
4. Сергеев Сергей. «Ивантеевский школьник получил срок за побоище». Коммерсантъ (2019), https://www.kommersant.ru/doc/3887763
5. «Детский Рунет». Институт исследований интернета (2019), www.internetinstitute.ru/portfolio/analytics/detskiy-runet-2019-otraslevoy-doklad/
6. «Подражательницы хабаровских живодерок имитировали истязания над котенком ради внимания». Комсомольская правда (2016), https://www.hab.kp.ru/daily/26614/3631208/
7. Baron, R.A. «The aggression-inhibiting influence of heightened sexual arousal». Journal of Personality and Social Psychology № 30 (1974)
8. Giannakopoulos, Theodoros. «Violence Content Classification Using Audio Features» (2006) Huesmann, Rowell. L. «The Impact of Electronic Media Violence: Scientific Theory and Research» (2007)
9. Michaud, Yves. «Les Cahiers Dynamiques». 2014/2 № 60 (2014)
10. Moore, H. «A Passion for Difference: Essays in Anthropology and Gender». Cambridge: Polity Press (1994)
11. «Online violence has real life consequences #ItIsMyBusiness». UNDP Serbia (2021), https://www.rs.undp.org/content/serbia/en/home/presscenter/articles/2021/digitalno-nasilje-ostavlja-stvarne-posledice.html
12. «Violence in the media: Psychologists study potential harmful effects». American Psychological Association (2013), https://www.apa.org/topics/video-games/violence-harmful-effects

18. Порнографический контент

Интернет считается ключевым каналом распространения порнографического контента. При этом дети и подростки могут сталкиваться с порнографией умышленно и неумышленно.

Умышленный поиск и потребление возможны из-за того, что механизмы верификации возраста в соцсетях и на сайтах с такого рода контентом несовершенны. Среди причин непреднамеренного столкновения с порнографией выделяют изучение смежных с сексом тематик, например, взаимоотношений между мужчиной и женщиной.

Это влияет на психическое здоровье и благополучие, в том числе столкновения с порнографией являются предиктором повышенной сексуальной агрессии и несерьезного отношения к сексуальным контактам.

Специфика риска

Порнография включает в себя книги, журналы, видео, фотографии и другие материалы, содержащие вульгарные, натуралистические и непристойные изображения половой жизни. Такие материалы не несут никакой художественной или академической ценности и служат только для сексуального возбуждения.

Несмотря на разнообразие исследований на эту тему, многие из них сильно ограничены в полноте ответов и в постановке вопросов.

Во-первых, сбор данных по вопросам сексуального характера у детей является сомнительным действием с точки зрения этики, особенно это касается младших возрастных групп.

Во-вторых, достоверность сведений, полученных от детей в ходе таких исследований, далека от совершенной, так как потребление порнографических материалов является порицаемым действием во многих культурах. Из-за этого у детей есть причины давать заведомо ложную информацию.

В-третьих, на исследования влияют многочисленные культурные, политические, законодательные и другие факторы, связанные с организацией, регионом, страной и прочими обстоятельствами, в которых проводится исследование.

В своем исследовании Антония Кадара, Алиссар Эль-Мур и Джо Лэтам, доктора австралийских университетов, приводят многочисленные примеры работ, которым приходилось менять методологию исследований в связи с обозначенными выше причинами.

В одной из своих работ доктор Йохен Петерс из Университета Амстердама называет интернет первоклассным инструментом для доступа к порнографии и подчеркивает, что анонимность, доступность и низкая стоимость доступа играют серьезную роль в проблеме потребления порнографии детьми. Сайтами в интернете пользуются и взрослые, и дети, — они приходятся друг другу соседями в самых разных сообществах. В результате такого соседства ситуация только усугубляется — при поиске в соцсетях по хештегу ребенок может получить доступ к порнографии. Таким образом, дети могут сталкиваться с порнографическим контентом умышленно и непреднамеренно.

Умышленный поиск и потребление возможны из-за того, что механизмы верификации возраста в соцсетях и на сайтах с такого рода контентом несовершенны. Попытка создать улучшенную систему в Великобритании вызвала большое количество критики — практика угрожает приватности пользователей и заставляет их оставлять больше данных посторонним компаниям.

Отдельными причинами непреднамеренного столкновения с порнографией являются изучение смежных с сексом тематик — медицины и здоровья, вопросов пубертата, романтических взаимоотношений. Ребенок может искать информацию о венерических заболеваниях и в процессе поиска случайно наткнуться на порнографический материал.

При встрече с порнографическими материалами часть детей испытывает отвращение, замешательство и тревогу, но эти ощущения становятся слабее с каждым столкновением.

Влияние на ребенка

Порнографический контент влияет на детей сразу в нескольких измерениях. Столкновение с ним, умышленное или неумышленное, может оказывать негативное влияние на знания и осведомленность о половом воспитании, вопросы здоровья, взгляды, отношение и ожидания по поводу пола и взаимоотношений с противоположным полом. Но существует разница в источнике последствий: часть из них связана с потреблением порнографии, а часть из них — результат того, какая порнография производится индустрией.

Порнографический контент оказывает влияние на психическое здоровье и благополучие, а столкновение с порнографией является предиктором повышенной сексуальной агрессии. Потребление и использование порнографии связано с более гедонистическим и менее серьезным отношением к сексуальным контактам. Кроме того, связь между потреблением порнографии и включением насилия в интимную жизнь существует у взрослых и соотносится с частотой потребления порнографии.

Отдельная проблема заключается не только в самом потреблении порнографии, но и в том, какая порнография производится и доминирует на рынке контента. В случае с порнографией, избыточная доля контента содержит проблематичные сигналы и смыслы. Порнографические нарративы о взаимоотношении полов, власти, удовольствии и выражении половой принадлежности являются гипертрофированной и порой гротескной формой реальности. В сценариях порнографии широко распространены сцены физического насилия, вербальные унижения, а согласие партнеров часто остается за рамками экрана. Дети не способны полностью осознавать весь контекст происходящего и отстранять насилие на экране от реальности, и они принимают эти формы девиантного поведения за норму.

Порнография является частью культуры и влияет на взгляды потребителей, и ущерб от нее по отношению к детям заключается не только в самом факте потребления контента. Ущерб усиливается и тем, какие именно материалы производит порноиндустрия. Из-за описанных выше особенностей потребление порнографии взращивает в ребенке ложные ожидания касательно половых актов, человеческого тела, норм поведения по отношению к своим партнерам. В одном из исследований, 44 % мальчиков от 11 до 16 лет признались в том, что на их сексуальные фантазии повлияла порнография. 20 % сказали, что порнография повлияла на их взгляды по поводу того, как себя должны вести женщины и мужчины. Поэтому у молодых людей активное использование порнографических материалов коррелирует с разочарованием в интимной жизни, сексуальной агрессией и неудовлетворенностью своим собственным телом.

Распространенность

Между ожиданиями родителей по поводу масштабов потребления порнографии детьми и реальной картиной есть существенная разница. Так, 83 % родителей сказали, что должны существовать более надежные способы подтверждения возраста, направленные на ограничение доступа детей к порнографии в интернете. 56 % детей в возрасте от 11 до 13 лет сказали, что они хотят, чтобы им был закрыт доступ к порнографическому контенту.

Отцы чаще полагали, что их ребенок видел порнографию (34 %), чем матери (19 %). При этом 75 % родителей ответили, что они не думают, что их дети смотрели порнографию. На самом деле 63 % детей и подростков в возрасте от 11 до 17 лет ответили, что они видели порнографические материалы намеренно или ненамеренно. В разрезе возрастов детей статистика выглядит так: 51 % детей в возрасте от 11 до 13 лет, 66 % детей в возрасте от 14 до 15 лет и 72 % подростков в возрасте 16-17 лет сказали, что они видели порнографию.

60 % родителей заявили, что они обсуждали с детьми порнографию, но куда меньше детей сказали, что их родители провели подобные беседы.

17 % родителей девочек ответили, что они считают, что их дочь видела порнографию. В случае с родителями мальчиков эта статистика составила 32 %. При этом 58 % девочек и 68 % мальчиков сказали, что они видели порнографию.

С просмотром порнографии негативная реакция ребенка постепенно снижается. Исследование с опросом детей об их ощущениях при столкновении с порнографией показало: наткнувшись на порнографию в первый раз, 17 % детей чувствуют возбуждение, 41 % чувствует любопытство, 27 % шокированы, 24 % в замешательстве. У тех, кто продолжает потреблять порнографию после первого опыта, реакция меняется следующим образом: 49 % испытывают возбуждение, 30 % чувствуют любопытство, 8 % шокированы, 4 % продолжают быть в замешательстве.

При этом 45 % детей признались в том, что они смотрели порнографию, чтобы узнать больше о половых контактах. Но лишь 24,5 % молодых людей в возрасте 18-24 лет назвали порнографию полезным ресурсом для этих целей.

Несмотря на нереалистичность сюжетов в порнографии, жестокость, сексизм и другие этические проблемы, 55 % мальчиков и 39 % девочек считали, что происходящее на экране реалистично.

Пример

Заявление Билли Айлиш (2021)

Будучи на радиошоу Howard Stern Show, 20-летняя певица Билли Айлиш призналась, что впервые ознакомилась с порнографией в 11 лет. Билли училась дома, поэтому у нее было много свободного времени и достаточно свободный доступ к компьютеру. Она рассказала о том, что просмотр порнографии позволял ей чувствовать себя более интересной и социально привлекательной. «Постоянный просмотр порнографии повредил моему сознанию, я чувствую, что сильно навредила себе», — объяснила певица. Она также рассказала, что из-за того, как порнография повлияла на ее взгляды, в первые несколько интимных контактов она не отказывала партнерам в вещах, в которых следовало бы отказать.

Источники

1. Панов В.П. и Х.Д. Аликперов. «Юридический словарь»
2. Bridges, A. J., et al. «Sexual Scripts and the Sexual Behavior of Men and Women Who Use Pornography. Sexualization, Media, and Society» (2016).
3. Jochen, Peter and Patti M. Valkenburg. «Adolescents' Exposure to Sexually Explicit Online Material and Recreational Attitudes Toward Sex» (2006)
4. Jochen, Peter and Patti M. Valkenburg. «Does exposure to sexually explicit Internet material increase body dissatisfaction? A longitudinal study» (2014)
5. Katz, Sherri Jean, et al. «Predicting Parent-Child Differences in Perceptions of How Children Use the Internet for Help With Homework, Identity Development, and Health Information» (2015)
6. Klaassen, Marleen J. E. and Peter Jochen. «Gender (In)equality in Internet Pornography: A Content Analysis of Popular Pornographic Internet Videos» (2014)
7. Martellozzo, E., et al. «I wasn't sure it was normal to watch it» (2016)
8. Morgan, Elizabeth M. «Associations between Young Adults' Use of Sexually Explicit Materials and Their Sexual Preferences, Behaviors, and Satisfaction» (2011)
9. Quadara, Antonia, et al. «The effects of pornography on children and young people» (2017)
10. Rothman, E.F., et al. «The Prevalence of Using Pornography for Information About How to Have Sex: Findings from a Nationally Representative Survey of U.S. Adolescents and Young Adults» (2021)
11. Vannier, Sarah A., et al. «Schoolgirls and Soccer Moms: A Content Analysis of Free «Teen» and «MILF» Online Pornography». (2014)
12. «BBFC Research into Children and Pornography». BBFC (2019)
13. «Billie Eilish says watching porn as a child "destroyed my brain"». The Guardian (2021), https://www.theguardian.com/music/2021/dec/15/billie-eilish-says-watching-porn-gave-her-nightmares-and-destroyed-my-brain
14. «UK online pornography age block triggers privacy fears». The Guardian (2019), https://www.theguardian.com/culture/2019/mar/16/uk-online-porn-age-verification-launch
15. «Young people, pornography & age-verification». BBFC (2020)

19. Дезинформация

Дезинформация — это попытка создать ложное впечатление и подтолкнуть объект воздействия к желаемым действиям или бездействию.

Это процесс манипулирования информацией, например, введение кого-либо в заблуждение путем предоставления неполной или вырванной из контекста информации, искажения части информации, распространения слухов, лжи и громких, но не подкрепленных фактами утверждений.

Дети не могут оценить достоверность информации, с которой они сталкиваются в интернете. Это может привести к формированию у них ложной картины мира, совершению некорректных действий по отношению к себе и окружающим.

Специфика риска

Интернет считается главным инструментом распространения дезинформации. В интернете дети могут свободно исследовать мироустройство, злободневные проблемы, получать информацию о событиях, собирать данные и делиться мнениями и опытом с другими. С ростом использования цифровых технологий увеличивается подверженность дезинформации. Дети могут быть особенно уязвимы к ложной информации, поскольку их мышление и когнитивные способности все еще развиваются, а психика очень неустойчива.

Опрос, проведенный ЮНИСЕФ в 10 странах, указывает на неспособность молодых людей оценивать информацию в интернете: 3 из 4 детей сообщили, что не могут оценить достоверность информации, с которой они сталкиваются в интернете. Исследование также показало, что дети из неблагополучных семей реже замечали сфабрикованный или вводящий в заблуждение контент, что свидетельствует о том, что семьи с низким уровнем образования и грамотности особенно подвержены риску. Исследователи пришли к выводу, что фейковые новости — это серьезная проблема для детей и молодежи, угрожающая их благополучию, доверию к журналистике и самой демократии.

Так, ЮНИСЕФ выделяет 7 видов дезинформации, причем первая категория является наименее вредной, а каждая последующая — более опасной:

1. сатира и пародия — дезинформация, созданная без намерения причинить вред, но способная обмануть читателя;
2. ложные связи в контенте — когда заголовки, прикрепленные цитаты и другие сопроводительные элементы не сочетаются с содержанием и смыслом контента;
3. правдивая информация, которая используется для того, чтобы пользователь сделал неверные выводы о проблеме или человеке;
4. правдивый контент, который сопровождается некорректно представленным контекстом, сопроводительный текст нацелен на то, чтобы изменить представление о правдивом факте;
5. контент, опирающийся на сфабрикованные и заведомо ложные источники;
6. контент, доля которого подвергнута манипуляции с целью обмана — результатом является частично ложная, частично правдивая информация;
7. сфабрикованный контент: полностью ложная информация, созданная для того, чтобы кому-то навредить или кого-то обмануть.

Мотивы

Причиной создания недостоверного контента могут быть различного рода мотивы: провокации, попытка журналистов выдать желаемое за действительное, обострение существующих конфликтов и усиление накала дискуссий, подрыв доверия к институтам государственной власти и в общем и целом — подогрев недовольства и эмоций.

В некоторых случаях сами дети, умышленно или нет, создают ложную информацию, распространяют и делятся ей. Такие приложения, как YouTube, TikTok и Instagram*, имеют широкую аудиторию несовершеннолетних, которые могут делиться контентом без ведома родителей. В поисках популярности и самоутверждения они публикуют сообщения в социальных сетях в надежде сделать что-то «вирусным». При этом дети не всегда распространяют дезинформацию только добровольно. Есть несколько задокументированных случаев, когда доверчивых подростков заставляли становиться первоисточниками преднамеренно ложной информации в интернете во время предвыборных кампаний или митингов.

Благодаря социальным сетям и интернету произошла дезинформационная революция. Мы живем в мире дешевых цифровых инструментов и сетей, которые есть в распоряжении не только государственных, но и негосударственных субъектов и частных лиц. От такой дезинформации исходит опасность, так как она косвенно влияет на резкие перемены настроения в обществе. Целенаправленную дезинформацию трудно распознать, поскольку события и новости иногда полностью придумываются автором, а порой намеренно вырываются из контекста, преувеличиваются, в результате чего у читателей формируется ложное представление. При этом речь не всегда идет о текстовом контенте: в сегодняшних условиях фотографии и видеоматериалы становятся все наиболее частым инструментом для манипуляций, так называемые дипфейки. Встречаются и другие разновидности дезинформации.

Дипфейки

Дипфейк — ветвь технологий для редактирования изображений, звуков и видео с помощью нейросетей. Английский термин происходит от слов «deep learning» и «fake», по сути означая подделку с использованием глубокого обучения.[8] Нередко дипфейки применяются для замены лица одного человека на лицо другого, более известного. Одной из особенностей технологии дипфейка является то, что в ней используются передовые методы машинного обучения и искусственного интеллекта для манипулирования или создания визуального и звукового контента с высокой степенью правдоподобности.

Компании из сферы информационной безопасности прогнозируют, что со временем число случаев распространения ложной информации с применением дипфейков будет расти. Дипфейки могут легко послужить инструментом для совершения онлайн-преступлений в отношении детей и повысить риски их прямого вовлечения в общий процесс распространения дезинформации в сети. Такого рода контент генерируется путем преобразования взрослых лиц в детские при помощи нейросетей и может использоваться для шантажа, а также затрудняет привлечение к ответственности преступников.

Несмотря на печальный опыт, технология дипфейка, в частности, может служить так же и для

[8] Глубокое обучение (англ. deep learning) — совокупность широкого семейства методов машинного обучения, основанных на имитации работы человеческого мозга в процессе обработки данных и создания паттернов, используемых для принятия решений.

благих целей. Дипфейки имеют ряд полезных функций для детей, модифицированные видеоизображения исторических персонажей, например, могут создаваться с целью обучения.

Астротурфинг

Астротурфинг — это маскировка искусственной общественной поддержки под настоящую. Чаще всего производится, чтобы придать легитимность и положительный контекст неэтичным или скандальным действиям корпораций и правительства. Само название является отсылкой к фирме Astroturf, которая производит искусственный газон для футбольных полей: оно сравнивает настоящее мнение общества с натуральной травой, а искусственно созданное — имитацией, синтетическим продуктом компании. Наемные работники, занятые астротурфингом, являются организованной силой, у них есть методическая поддержка. Интернет для таких работников — площадка, на которой они создают видимость общественного мнения. Каждый из них может имитировать сразу несколько человек и координировать действия с другими работниками.

Газлайтинг

Газлайтинг — тип психологического насилия, направленный на формирование у жертвы чувства искусственного сумасшествия, мнимой дезориентации и сомнения в собственной реальности через постоянные обесценивающие шутки, обвинения и запугивания. Сегодня газлайтинг становится все более распространенным термином, используемым для описания стратегий манипулирования сознанием особо впечатлительных людей. Данный инструмент применяется как в политике, где психологическая манипуляция доминирует в современной эпохе «постправды»[9], так и в межличностных отношениях. В уголовный кодекс Великобритании ответственность за газлайтинг официально включили в 2015 году — с тех пор более 300 человек были обвинены в этом преступлении. У газлайтинга есть множество приемов, большинство из них заключаются в распространении вводящей в заблуждение и манипулятивной информации с целью дестабилизировать и дезориентировать общественное мнение по политическим вопросам.

Проверка фактов

Проверка фактов логически относится к тематике дезинформации и сопротивления манипуляции. Фактчекинг — это практика систематической публикации оценки обоснованности заявлений, сделанных государственными должностными лицами и учреждениями, с попыткой определить, являются ли утверждения фактическими.

Если информация исходит от одного человека, это личное мнение, а не факт. Зачастую ребенку с его несформировавшейся психикой и острой восприимчивостью трудно понять, передает ли автор статьи выводы ученых или пытается навязать ему свою радикальную позицию по отношению к волнующей ребенка проблеме.

Исследования неизменно показывают, что исправления, вносимые специалистами и искусственным интеллектом, уменьшают степень доверия пользователей к дезинформации и снижают вероятность ее распространения среди людей. Часть людей подозревают организации, занимающиеся проверкой фактов, в дезинформации, особенно когда вопрос окружен политическим контекстом. У таких организаций идеальная позиция, чтобы служить своим собственным интересам — некоторые исследования показывают, что разные организации фактчекеров могут давать противоположные оценки одной и той же новости.Кроме

[9] Постправда (англ. post-truth) — обстоятельства, при которых объективные факты являются менее значимыми при формировании общественного мнения, чем обращения к эмоциям и личным убеждениям.

того, сама эффективность этой практики разнится от исследования к исследованию. Для того чтобы уберечь детей от воздействия фейкового контента, в школах рекомендуется обучать критическому мышлению и цифровой грамотности, поскольку эти черты помогают развивать способность детей выявлять ложь среди новостей и более уважительно взаимодействовать друг с другом в интернете.

Распространенность

Во время пандемии COVID-19 почти 80 % пользователей интернета в США сообщили, что видели фальшивые новости о вспышке коронавируса, где намеренно подчеркивался масштаб проблемы. Более того, около 52 % американцев регулярно сталкиваются с фейковыми новостями в интернете. Примерно половина взрослых американцев (48 %) заявляют, что правительство и технологические компании должны принять меры для ограничения ложной информации. При этом в ухудшение ситуации с фейковыми новостями верят 56 % жителей, в то время как в положительный исход борьбы — лишь 10 %.

В США подростки в возрасте от 13 до 17 лет чаще узнают новости из социальных сетей или YouTube, чем из новостных организаций, а 60 % подростков, получающих новости с YouTube каналов, говорят, что они каждый день узнают о событиях от знаменитостей, инфлюенсеров и непроверенных источников. Многие дети подражают блогерам, за которыми они следят, поэтому с легкостью соглашаются с их мнением по отношению практически ко всем жизненно важным вопросам, а порою их доверие становится настолько чрезмерным, что дети охотно делятся фейковой информацией среди сверстников в сети и запускают механизм ее распространения.

Чаще всего целенаправленное распространение ложной информации встречается в социальных сетях. По сообщению NBC News, во втором квартале 2020 года Facebook* удалила около 7 млн постов, содержащих провокационные высказывания, а также фейковые новости о пандемии и экстремизме. С начала пандемии и до апреля 2021 года Facebook* и Instagram* пометили 167 млн сообщений как подозрительные и требующие проверки на достоверность.

Примеры

Как стать феей огня (2016)

В 2016 году в различных соцсетях дети делились инструкцией с изображением героев из популярного мультфильма о феях Винкс (Winx). Изображение сопровождалось инструкцией «как стать феей огня в домашних условиях». Рассылку получили дети младшего возраста от 5 до 8 лет.

В 2016 году пятилетняя Соня Подольская попыталась следовать инструкции и с помощью газовой плиты превратиться в фею огня. В квартире произошел пожар, а девочка получила ожоги третьей степени.

Автором инструкции был несовершеннолетний Азаров Алексей, администратор сообщества о феях Винкс. Он создал эту картинку ради шутки, но позже признал свою ошибку.

Смерть любимого актера (2018)

13-летняя Хлоя увидела новость о предполагаемой смерти любимого актера Сильвестра Сталлоне. Девочка подумала, что это правда, и поделилась этим с членами семьи. Многие люди были очень расстроены. Но новость оказалась фейковой.

Когда появилась правда о том, что Сильвестр Сталлоне был жив и здоров, Хлоя сказала, что чувствовала себя глупо. «Мне следовало подробнее изучить информацию, прежде чем ее публиковать», — добавляет она. Таким образом, фейковые новости могут сделать детей более обеспокоенными, нанести ущерб их самооценке и исказить их мировоззрение.

Альянс австралийских Ритейлеров (2010)

Альянс австралийских ритейлеров — организация, в которую входят владельцы киосков и магазинов при заправках. Альянс протестовал против антитабачного проекта, который разрабатывался правительством Австралии. Конечной целью проекта была идея заставить производителей сигарет изменить дизайн пачек: стирать брендовые маркировки, помещать на пачки предупреждения о вреде здоровью и так далее. Альянс состоял из нескольких ассоциаций и был сформирован именно для того, чтобы противостоять проекту. Организация закупала страницы в газетах и политически направленную рекламу, причем во всех случаях она оспаривала проект с точки зрения рядовых работников и владельцев малого бизнеса.

Оказалось, что альянс спонсировался компанией Phillip Morris, международным производителем сигарет. Попытка манипуляции общественным мнением была признана астротерфингом, и альянс начал разваливаться — из него уходили члены, а общественное доверие упало.

Источники

1. Немцева Мария. «Вооруженный глаз: как распознать дипфейк». Известия (2021), iz.ru/1137510/mariia-nemtceva/vooruzhennyi-glaz-kak-raspoznat-dipfeik
2. Пашенцев Евгений и др. «Злонамеренное использование искусственного интеллекта в Северо-Восточной Азии и угрозы международной информационно-психологической безопасности». Государственное управление. Электронный вестник 80 (2020)
3. Смирнов А. А. «Глубокие фейки. Сущность и оценка потенциального влияния на национальную безопасность». Свободная мысль 5 (1677) (2019): 63-84
4. «Борьба с дезинформацией: укрепление цифровой устойчивости Североатлантического союза», Johns Hopkins University, Imperial College London & Georgia Institute of Technology, NATO REVIEW (2021)
5. «Пятилетняя девочка хотела стать феей Винкс и подожгла себя». Служба новостей pg12.ru (2016), https://pg12.ru/news/23574
6. Ahern, Kathy. «Institutional betrayal and gaslighting». The Journal of perinatal & neonatal nursing 32.1 (2018): 59-65.
7. Bhabha, Jacqueline. «The child—what sort of human?». PMLA/Publications of the Modern Language Association of America 121.5 (2006): 1526-1535.
8. Bradshaw, Bailey and Howard. «Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation». University of Oxford (2021)
9. Burns, By Judith. «Fake News Harms Children’s Self-Esteem and Trust, Say MPs». BBC News (2018)
10. Chen, Xinran, et al. «Why Students Share Misinformation on Social Media: Motivation, gender, and study-level differences». Journal of Academic Librarianship.
11. Cho, Charles H., et al. «Astroturfing Global Warming: It Isn’t Always Greener on the Other Side of the Fence» (2011)

12. Howard, Philip N., et al. «Digital misinformation/disinformation and children». UNICEF (2021)
13. Jarman, Jeffrey W. «Influence of Political Affiliation and Criticism on the Effectiveness of Political Fact-Checking» (2016)
14. Keller, Franziska B., et al. «Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign» (2019)
15. Kietzmann, Jan, et al. «Deepfakes: Trick or treat?» Business Horizons 63.2 (2020): 135-146.
16. Livingstone, Sonia, et al. «Global kids online comparative report» (2019)
17. Mikhailova, Anna. «Theresa May Pledges to Tighten the Law on “Gaslighting” Abuse». The Telegraph (2018), https://www.telegraph.co.uk/politics/2018/05/23/theresa-may-pledges-tighten-law-gaslighting-abuse/
18. Mitchell, Amy and Mason Walker. «More Americans Now Say Government Should Take Steps to Restrict False Information Online than in 2018». Pew Research Center (2021)
19. Nieminen, Sakari and Lauri Rapeli. «Fighting Misperceptions and Doubting Journalists’ Objectivity: A Review of Fact-checking Literature» (2018)
20. Rinehart, Aimee. «Fake News. It’s Complicated» (2021)
21. Shah, Sabir. «Interesting Statistics about Fake News on Social Media». The News International (2021), https://www.thenews.com.pk/print/893091-interesting-statistics-about-fake-news-on-social-media
22. Starbird, Kate, et al. «Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations». Proceedings of the ACM on Human-Computer Interaction 3.CSCW (2019): 1-26
23. Suciu, Peter. «Spotting Misinformation On Social Media Is Increasingly Challenging». Forbes (2021), https://www.forbes.com/sites/petersuciu/2021/08/02/spotting-misinformation-on-social-media-is-increasingly-challenging/
24. Sweet, Paige L. «The sociology of gaslighting». American Sociological Review 84.5 (2019): 851-875.
25. Tolosana, Ruben, et al. «Deepfakes and beyond: A survey of face manipulation and fake detection». Information Fusion 64 (2020): 131-148.
26. Vaccari, Cristian and Andrew Chadwick. «Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news». Social Media+ Society 6.1 (2020)
27. Vosoughi, Soroush, et al. «The spread of true and false news online». Science 359.6380 (2018): 1146-1151
28. Vziatysheva, Victoria. «How fake news spreads online?» International Journal of Media and Information Literacy 5 (2020): 217-226.
29. Walter, Nathan, et al. «Fact-checking: A meta-analysis of what works and for whom». Political Communication 37.3 (2020): 350-375
30. Watson, Amy. «Fake News in the U.S. — Statistics and Facts». Statista (2021), https://www.statista.com/topics/3251/fake-news/
31. Westerlund, Mika. «The emergence of deepfake technology: A review». Technology Innovation Management Review 9.11 (2019)
32. «10 Fake Grassroots Movements Started By Corporations To Sway Your Opinion». Insider (2011), https://www.businessinsider.com/astroturfing-grassroots-movements-2011-9
33. «Big tobacco bankrolls anti-Labor ad campaign». ABC News (2010), https://www.abc.net.au/news/2010-08-04/big-tobacco-bankrolls-anti-labor-ad-campaign/931280
34. «Fake news worldwide — statistics & facts». Statista (2021), https://www.statista.com/topics/6341/fake-news-worldwide/#dossierKeyfigures
35. «Interesting statistics about fake news on social media». The International News (2021)
36. «Retail group quits cigarette label campaign». ABC News (2010), https://www.abc.net.au/news/2010-08-11/retail-group-quits-cigarette-label-campaign/939914
37. «Voters Don’t Trust Media Fact-Checking». Rasmussen Reports (2016)

38. «What is disinformation». Bundesregierung. Startseite, German Federal Government (2021)
39. «Why Generation Z Falls for Online Misinformation». MIT Technology Review (2021)

20. Опасные тренды и челленджи

Тренды и челленджи вовлекают детей и подростков в массовые активности, которые могут угрожать психическому и физическому здоровью участников или окружающих, через социальные сети и обмен сообщениям в мессенджерах.

Вовлечение происходит путем приглашения аудитории в игру или соревнование с выполнением заданий, отчетами в фото- и видеоформате или онлайн-трансляции.

Среди последствий опасных трендов могут быть отравления, физические и психологические травмы, нанесенные себе и другим, и даже непреднамеренный летальный исход или суицид. Кроме того, опасные тренды могут способствовать сексуализации детей или вовлекать их в криминальные сообщества.

Специфика риска

Один из наиболее ярких примеров опасных трендов — **челленджи** (от англ. challenge — вызов, сложная задача на выполнение). Это приглашение к выполнению определенного задания, повторению действий с последующей публикацией информации об этом в социальной сети и вовлечением зрителей в активность. Челленджи имеют игровой и соревновательный характер. Если же в челлендже предлагается преодолеть себя, свой стыд, пренебречь общественными нормами и сделать что-то на публику, это можно определить как фаршинг — неформальное направление интеллектуального и психологического экстрима. Фаршинг включает в себя риск, который заставляет экспериментировать с границами дозволенного, нарушать нормы этики и морали.

Помимо этого, выделяют челленджи-мистификации (Hoax) — вид опасных челленджей, основанных на мистике и ложной информации, вызывающей испуг, панику и психологическую травму. Также опасными являются маргинальные тренды, когда в режиме онлайн-трансляции блогеры выполняют задания зрителей. Для этого часто создаются закрытые группы в соцсетях «ВКонтакте», «Одноклассники», Facebook*, где проводятся игры, связанные с самоповреждающими или агрессивными действиями.

Мотивация

Интерес детей и подростков к участию в подобных акциях продиктован спецификой их возраста. Дети от 4 до 12 лет очень доверчивы, а их критическое мышление и чувство опасности еще не развито.

Для подростков социальные сети и онлайн-общение с другими — это возможность проявить себя, примкнуть к новой группе, получить социальное одобрение в виде лайков и стать популярным. Получение лайков за отчеты о выполненных заданиях создают у подростка чувство победы, сопряженное с самоудовлетворенностью. Для несовершеннолетних одобрение имеет решающее значение в процессе развития личности. Их самооценка растет, поскольку они чувствуют себя участниками чего-то большего и разделяют некий общий опыт, который можно обсуждать с друзьями.

Желание получить признание от сверстников может отключить рациональное мышление и не оставить места для мыслей о возможном вреде или риске. Именно это мотивирует подростков делать опасные селфи и видео. Давление группы также может сподвигнуть на компромиссы с риском для себя. В целом люди более склонны к рискованному поведению, когда они находятся в группе и действуют заодно. Это напрямую имеет отношение к подросткам, потому что именно

в этом возрасте общение со сверстниками имеет большое значение. Подростки чаще совершают правонарушения, будучи в компаниях.

У детей и подростков развит инстинкт познания, исследования нового. Поэтому задания в форме игры «посмотри, что получится» и эксперименты с возможностью поделиться результатами с друзьями, также снижают восприятие возможного риска.

Последствия опасных трендов

В большинстве случаев участие в выполнении задач или в игре приводят к опасным последствиям из-за непонимания реального риска и несформировавшегося критического мышления. Если подростки уже имеют какие-либо психологические проблемы, в том числе суицидальные наклонности, они находят опасные тренды, усугубляющее состояние, что в совокупности является причиной трагедии.

Игры и челленджи впоследствии могут привести к деструктивному поведению подростка, в том числе спровоцировать агрессию, участие в деятельности экстремистских сообществ, популяризировать криминальное поведение, алкоголь и психоактивные вещества, суицидальное поведение и негатив по отношению к окружающим.

Непреднамеренный летальный исход. Суть челленджа #BlackoutChallenge — доведение себя до обморока путем задержки дыхания, #PassOutChallenge — доведение себя до обморока мотанием головой. Челлендж-мистификация «Момо»: в WhatsApp участникам приходили экстремальные задания, связанные с риском для психики и жизни. В этом челлендже произошло более 10 самоубийств среди подростков в возрасте от 9 до 18 лет.

Самоповреждения. Челлендж «Соль и лед»: необходимо посыпать руку солью и положить сверху несколько кусочков льда. Соль вступает со льдом в реакцию, и температура резко падает до -17 ℃. Участников убеждают терпеть боль как можно дольше, что приводит к обморожению и некрозу тканей.

Отравления. Челлендж «40 таблеток»: участники пьют 40 таблеток дротаверина, что оборачивается отравлением и передозировкой.

Травмы и увечья себе и другим. Челлендж #MilkCrateChallenge: нужно забраться на пирамиду из пластиковых ящиков. Из-за участившихся травм TikTok блокирует челлендж. Суть #SkullBreaker, #TrippingJump: двое участников сбивают с ног ничего не подозревающую жертву таким образом, чтобы та ударилась затылком или спиной об пол. В результате чего дети могут потерять сознание или получить сотрясение головного мозга, множественные переломы.

Суицид. Серии игр с суицидальным финалом: «Синий кит», «Тихий дом», «Разбуди меня в 4:20», «Млечный путь», F57, NaN.

Психологические травмы. Цепочечные письма с ужасающим содержанием: согласно инструкции, если не переслать это письмо, ждет «смерть всей семьи», а при отправке всего 15 таких писем — «смерть мамы». Текст рассылки создает психологическую травму у детей младшего и среднего школьного возраста, они часто верят в это и пересылают сообщение друзьям.

Вовлечение в асоциальную, противоправную или криминальную деятельность. Содержание #OutletChallenge: участники вставляют в розетку лишь часть вилки со шнуром от телефонного зарядного устройства, после чего пытаются вызвать искру, прикоснувшись

монетой к железной вилке. Из-за данного челленджа происходили пожары в школах и торговых точках, инициаторам возгорания были предъявлены уголовные обвинения.

Сексуализация детей. Акция от паблика в «ВКонтакте», в которой за фото в купальнике у новогодней елки с табличкой с названием паблика в руках обещали заплатить участникам 1000 рублей, а победителю — 3000 рублей. В акции участвовали подростки, их фотографии были опубликованы.

Челлендж #SilhouetteChallenge: нужно опубликовать танец, наложив специальный фильтр, чтобы был виден один силуэт. Танцы проходят как в обнаженном или полуобнаженном виде, так и с детскими персонажами. Поскольку в челлендже смешанная аудитория, дети могут увидеть неприемлемый контент. Несовершеннолетние девушки также участвуют в челлендже. Однако есть способы убрать фильтр, вследствие чего участницы подвергаются риску публикации и публичного обсуждения исходных видео без их согласия.

Распространенность

В 2021 году специалисты TikTok, объединившись со специалистами по безопасности, изучили влияние челленджей на молодежь. В исследовании принимали участие 10 000 человек из 10 разных стран мира. По итогу 48 % несовершеннолетних сочли челленджи безопасными, 32 % рассказали, что заметили возможную опасность, но отметили, что в целом челлендж был безопасным, а 14 % сразу заявили о больших рисках. Помимо этого, 3 % сказали, что последний челлендж, который они видели, был очень опасным.

Наиболее опасным для жизни и здоровья подростков большинство родителей (93 %) считают свободную доступность к контенту, несущему суицидальные призывы, призывы к насилию, пропагандирующему наркотики и подобные нелегальные и опасные для здоровья вещи.

40 % школьников также уверены, что интернет-среда иногда опасна. Значительная часть из них получила в интернете негативный опыт. Однако треть подростков в возрасте 14-15 лет и чуть больше трети (37 %) подростков 16-17 лет считают, что интернет не опасен.

Примеры

#NutmegChallenge (2020)

#TutmegChallenge (челлендж «Мускатный орех») набирал в TikTok 46,4 млн просмотров.
Он заключается в том, что дети проглатывают большое количество мускатного ореха в попытке испытать галлюцинации. Токсичность мускатного ореха связана с маслом миристицина.
Однако в инструкции к челленджу не указывается дозировка, которая приводит к отравлениям (1-4 чайных ложки). Симптомы отравления (тахикардия, тошнота, рвота), которые появляются в течение 3-6 часов и продолжаются 12-24 часа.

#TidePodChallenge (2018)

Флешмоб заключался в глотании на камеру капсул для стирки — компактные капсулы с моющим веществом похожи на конфеты. Большинство участников снимали ролики, но не глотали капсулы. Однако такие видео повлияли на впечатлительных детей.

В 2017 году центры токсикологического контроля получили сообщения о более чем 10 500 случаях отравления подобными веществами детьми младшего возраста.

Источники

1. Жильцова Дина. «"Газовая Фея" и "Кровавая Мери": Как защитить ребенка от интернет-спама». РИАМО (2017), riamo.ru/article/199877/gazovaya-feya-i-krovavaya-meri-kak-zaschitit-rebenka-ot-internet-spama.xl
2. Калинина Наталья. «Риски и угрозы современной интернет-среды и их профилактика среди несовершеннолетних». Всероссийский вебинар: «Профилактика суицидального поведения детей и подростков, связанного с влиянием сети Интернет» (2017)
3. Мазанов Артём. «Флешмоб: Tide Pod Challenge». TJ (2018), tjournal.ru/internet/64899-fleshmob-tide-pod-challenge
4. Макаренко В. «На смену "китам и бабочкам" пришли "лёд и соль"» Комсомольская правда. Украина (2017), https://kp.ua/incidents/579584-na-smenu-kytam-y-babochkam-pryshly-led-y-sol
5. Мирончук Роман. «Выпейте 40 таблеток и посмотрите, что будет: в сети распространяется смертельный челлендж». РБК-Украина (2021)
6. Соболева А.Н. «Риски интернет-пространства для здоровья подростков: возрастной и гендерный анализ». АНО «ЦНПРО», № 1 (2016)
7. Солдатова Г. В. и др. «Пойманные одной сетью». Социально-психологическое исследование восприятия интернета детьми и подростками–М (2011)
8. Солдатова Г. У. и др. «Мы в ответе за цифровой мир: Профилактика деструктивного поведения подростков и молодежи в Интернете» (2019)
9. Шевченко Марина. «Смертельные селфи: почему дети рискуют жизнью ради лайков». Vesti.ua (2018), vesti.ua/lite/health/300938-smertelnye-selfi-pochemu-deti-riskujut-zhiznju-radi-lajkov
10. «Жертва МОМО — в Киеве школьница пыталась покончить собой в День знаний». Vesti (2018), vesti.ua/kiev/301345-zhertva-momo-v-kieve-shkolnitsa-pytalas-pokonchit-soboj-v-den-znanij
11. «Комплексная программа профилактики деструктивного поведения в интернете у подростков и молодежи». Фонд развития интернета и Московский институт психоанализа (2019)
12. «Монетизация страха и ненависти: в России хотят запретить треш-тримы». ТВЦ (2021), https://www.tvc.ru/news/show/id/219056
13. Atherton, Rachel Rose. «The Nutmeg Challenge: a dangerous social media trend». Archives of disease in childhood 106.5 (2021)
14. Brion-Meisels G., et al. «Exploring effective prevention education responses to dangerous online challenges». (2021)
15. Brunick, Kaitlin L., et al. «Children’s future parasocial relationships with media characters: The age of intelligent characters». Journal of Children and Media 10.2 (2016): 181-190.
16. Garvey, Marianne. «Conan O'Brien's tweet prompts FDA to discourage #MilkCrateChallenge». CNN (2021), https://edition.cnn.com/2021/08/24/entertainment/milk-crate-challenge-fda-trnd/index.html
17. Gordon, Lauren. «Moms Need to Warn Their Daughters About the Silhouette Challenge». Cafemom (2021), cafemom.com/parenting/silhouette-challenge/on-youtube-there-are-still-currently-dozens-of-tutorials-on-how-to-remove
18. Hahn, Jason Duaine. «10-Year-Old Girl Dies Trying “Blackout Challenge”from Social Media, Mom Says». PEOPLE (2021), people.com/human-interest/10-year-old-girl-dies-trying-blackout-challenge-from-tiktok
19. Konrad, Kerstin, et al. «Brain development during adolescence: neuroscientific insights into this developmental period». Deutsches Ärzteblatt International 110.25 (2013)
20. McCarthy, Christine. «Concerns over TikTok Silhouette Challenge Exposing More than Users Intended». Boston 25 News, (2021),

www.boston25news.com/news/local/concerns-over-tiktok-silhouette-challenge-exposing-more-than-users-intended/UPPA6RVIONFDRGTBKZL7N4DOPA
21. Pescaro, Mike. «TikTok Outlet Challenge: 2 Students Being Charged After 8 Outlets Damaged at Mass. School». NBC10 Boston (2020), https://www.nbcboston.com/news/local/tiktok-outlet-challenge-2-students-being-charged-after-8-outlets-damaged-at-mass-school/2068830/
22. Stoner, James A. F. «Risky and cautious shifts in group decisions: The influence of widely held values». Journal of Experimental Social Psychology (1968)
23. Suwastini, Ni Komang Arie, et al. «The dangerous trend among teenagers analyzed: social media as academic research». The fourth International Conference on English across cultures (2018)
24. Wakefield, By Jane. «TikTok Skull-Breaker Challenge Danger Warning». BBC News (2020), www.bbc.com/news/technology-51742854
25. «Massachusetts Students Face Criminal Charges after Viral “Outlet Challenge”Damages School». New Bedford Guide (2020), www.newbedfordguide.com/massachusetts-viral-outlet-challenge/2020/01/29.
26. «TikTok публикует результаты глобального исследования об онлайн-челленджах и их влиянии на подростков». TikTok (2021), https://newsroom.tiktok.com/ru-ru/dangerous-challenges-and-hoaxes-report-2021-russia
27. «Why kids love TikTok Challenges». Psychology Today (2021), https://www.psychologytoday.com/us/blog/positively-media/202102/why-kids-love-tiktok-challenges

Группа 6. Аддикция, формирование зависимости от интернет-среды

К этой группе относятся риски, при наступлении которых у ребенка формируется зависимость от интернета в целом или конкретных его элементов, например: алгоритмы удержания внимания, игровая зависимость и избыточное использование интернета.

Последствия таких рисков заключаются в ухудшении общего самочувствия ребенка, его социальных связей, успеваемости. Нередко подобная зависимость приводит к отклонениям в поведении, отсутствию интереса к привычной жизни и депрессии.

21. Алгоритмы удержания внимания

Алгоритмы анализируют реакции пользователя, считывают моментальный отклик на информацию, а затем подбирают похожий контент. Таким образом они ограничивают поток информации до интересных пользователю публикаций, формируют рекомендации, показывают таргетированную рекламу.

Основная цель алгоритмов — удерживать внимание ребенка как можно дольше. Для этого используется множество маркетинговых инструментов, например, игровые петли, создающие эффект незавершенности действия и вызывающие синдром упущенных возможностей.

Показывая только то, что интересно пользователю, алгоритмы изначально проектируются на поляризацию мнений на любые темы, которые влияют на становление мировоззрения детей и подростков.

Специфика риска

Эффективность алгоритмов зависит от полноты и точности данных о пользователе, его активности и предпочтениях. Их основная задача — как можно дольше удерживать внимание, тем самым увеличивать время активности на сайте или в приложении.

Социальные платформы привлекают специалистов по когнитивной психологии, поведенческой экономике и нейронауке для разработки методов удержания внимания и увеличения времени пользовательских сессий. За основу принципов работы алгоритмов взяты методы, аналогичные методам игорного бизнеса.

Методы, заложенные в алгоритмах

Бывший сотрудник Facebook* назвал алгоритмы соцсети «дофаминовыми петлями быстрой обратной связи». Одобрения в виде лайков, просмотров, комментариев — это легкие, мгновенные стимулы-поощрения, вызывающие всплеск дофамина. Каждый пользователь социальной сети поощряет в этом другого. При этом подростки в возрасте от 10 до 14 лет наиболее восприимчивы к немедленному вознаграждению.

Игровые петли (ludic loops) создают ситуацию, в которой пользователь чувствует незавершенность действия, возникает непреодолимое желание постоянно следить за новостями и уведомлениями, возвращаться в соцсеть как можно чаще.

Отсутствие сигналов остановки провоцирует тревожность и стресс из-за возможности упустить поощрение, этот эффект называют **синдромом упущенных возможностей** (FOMO). Исследование, проведенное среди подростков, выявило их особую уязвимость к этому синдрому. Это дополняется принципом **прерывистого подкрепления** — эффект непредсказуемости вознаграждения, которое усиливает вовлечение в игровую петлю и еще больше провоцирует тревогу.

Алгоритм преследования включается тогда, когда по некоторым признакам поведения пользователя был определен небольшой интерес или эмоциональный отклик, но активность не была завершена. Для детей такое преследование может вызвать риск навязывания рекламы, неподходящего или травмирующего контента, которые ранее были проигнорированы.

Персональные рекомендации показывают только то, что человек хочет увидеть, ограничивают его узкими, похожими интересами. Такое ограничение не позволяет получить объективную оценку или услышать другое мнение. В итоге каждый пользователь начинает существовать в своем информационном пузыре, который влияет на формирование мнения, интересов, привычек, мировоззрения – **«пузырь фильтров»**. Кроме того, мнение большинства, выраженное в группе, может сформировать взгляды ребенка. Алгоритм TikTok создает пузырь фильтров исходя из внешности, пола, возраста и расы, рекомендуя профили, внешне похожие на ранее просмотренные.

Алгоритмы направляют внимание пользователя на рекомендации, подбирают людей по интересам и убеждениям, таким образом люди объединяются в группы. Этот эффект называется **«эхо-камера»**, когда пользователь окружен только той информацией и теми людьми, которые подтверждают одну точку зрения, подкрепляют их правоту.

Эффекты и последствия

Длительные сессии вырабатывают привычки и постепенно влияют на перестройку когнитивных функций. При возникновении зависимости это влияет на анатомическое изменение строения мозга. Дети и подростки наиболее уязвимы к этому, так как их мозг находится в процессе развития, а контроль импульсов еще недостаточно развит. Увеличение экранного времени у детей и подростков повышает риск появления синдрома дефицита внимания и гиперактивности, нарушения концентрации.

Алгоритмы изначально проектируются на наращивание интенсивности и эскалации на любые темы, в том числе касающиеся социальных, гендерных, политических аспектов, которые влияют на становление мировоззрения детей и подростков. Но алгоритмы работают не идеально, и случаются ошибки, из-за которых в рекомендации зачастую попадает неподходящий для детей, травмирующий контент. Одно из недавних исследований показало, что дети в возрасте до трех лет с вероятностью 45 % нажимают на неприемлемый контент в YouTube Kids всего в десяти рекомендованных видеороликах.

Алгоритмы подбора контента и групп общения влияют не только на убеждения, но и психоэмоциональное состояние. Принципы повышения эмоционального отклика и объединения в группы используют склонность людей к спорам и конфликтам. Так алгоритмы способствуют поляризации внутри социальной сети — создаются противоборствующие группы, которые проводят длительное время в спорах, провоцируют конфликты, вовлекаются в политическую деятельность или экстремистские группировки.

Сотрудница Facebook*, социолог Моника Ли отмечала, что алгоритмы платформы несут ответственность за рост количества экстремистских сообществ: «64 % всех новых подписчиков экстремистских групп пришли из рекомендаций».

Распространенность

По данным исследований, в России до 45 % восьмилетних детей проводят за экраном более 2 часов в день, в то время как у 16-летних этот показатель достигает почти 80 %. Некоторые исследования показывают, что подростки проводят около 9 часов в день в интернете. В США с 2011 по 2017 год среди детей время, проведенное за экраном, увеличилось в 10 раз.

Особые опасения вызывает снижение возраста пользователей социальных сетей. Исследование по использованию YouTube среди детей от 1 до 4 лет показало, что дети проводят время на платформе уже в младенчестве. А к восьми годам дети с высокой вероятностью проводили наибольшее количество времени у экрана, если занимались домашними делами, помогали родителям с младшими братьями и сестрами. Увеличение экранного времени у детей связано с неврологическими показателями задержки созревания, изменений в развитии мозга и слабого вербального интеллекта.

Пример

Алгоритмы Tik-Tok, Instagram* и Facebook* (2021)

В июле 2021 года 5Rights Foundation провели исследование, в ходе которого создали профили в TikTok, Instagram* и Facebook*, опираясь на данные реальных подростков от 13 до 17 лет, и имитировали их активность.

Согласно отчету, уже через несколько часов после создания учетных записей рекомендательный алгоритм предлагал неприемлемый и травматичный контент.
Также была показана таргетированная реклама, содержащая контент с возрастным ограничением 18+. Через несколько часов после регистрации с экспериментальными профилями связались неизвестные взрослые, которых система ранжирования выводила в рекомендации.

Одна учетная запись, созданная на имя 17-летней девушки, лайкнула пост от бренда спортивной одежды о диете. Затем она подписалась на аккаунт, который ей предложили после публикации фотографии «путешествия до и после похудения». Этих двух действий было достаточно, чтобы алгоритм сформировал поток контента, в котором рассказывали про диеты и показывали фотографии моделей, многие из которых были отредактированы. Для подростков это может сформировать комплексы по поводу фигуры и недостижимый образ идеала тела.

Также эксперимент показал, что алгоритмы интерпретируют любые действия, в том числе настроение на фотографиях, для дальнейших рекомендаций. Так, если алгоритм определит настроение аватара как грустное или депрессивное, то может создать ленту в соответствии с данным определением и усилить этот эффект.

Источники

1. Эяль Нир и Райан Хувер. «Покупатель на крючке». Руководство по созданию продуктов, формирующих привычки (2014)

2. «Экранное время в жизни школьника». ФБУЗ “Центр гигиенического образования населения” (2021), http://cgon.rospotrebnadzor.ru/content/62/4107
3. Alter, Adam. «Irresistible: The rise of addictive technology and the business of keeping us hooked». Penguin (2017)
4. Anderson, Jenny. «American Kids’ Daily Mobile Screen Time Is Almost 10 Times Higher than It Was in 2011» (2017)
5. Beyens, Ine, et al. «I don’t want to miss a thing: Adolescents’ fear of missing out and its relationship to adolescents’ social needs, Facebook use, and Facebook related stress». Computers in Human Behavior 64 (2016)
6. Cherry, Kendra. «What is operant conditioning and how does it work?» How reinforcement and punishment modify behavior. Verywell Mind (2019)
7. Crone, Eveline A. and Elly A. Konijn. «Media use and brain development during adolescence». Nature communications 9.1 (2018)
8. Del Vicario, Michela, et al. «Echo chambers: Emotional contagion and group polarization on facebook». Scientific reports 6.1 (2016)
9. Dubicka, Bernadka, et al. «Screen time, social media and developing brains: a cause for good or corrupting young minds?» Child and Adolescent Mental Health 24.3 (2019)
10. Dunckley, Victoria L. «How the Tech Industry Uses Psychology to Hook Children». Psychology Today (2018), www.psychologytoday.com/us/blog/mental-wealth/201810/how-the-tech-industry-uses-psychology-hook-children
11. Edwards, Haley Sweetland. «You’re addicted to your smartphone. This company thinks it can change it». Time (2018), https://time.com/5237434/youre-addicted-to-your-smartphone-this-company-thinks-it-can-change-that/
12. Falk, Emily and Christin Scholz. «Persuasion, influence, and value: Perspectives from communication and social neuroscience». Annual review of psychology 69 (2018)
13. Ferster, Charles B. and Burrhus Frederic Skinner. «Schedules of reinforcement». (1957)
14. Gretzel, Ulrike and Daniel R. Fesenmaier. «Persuasion in recommender systems». International Journal of Electronic Commerce 11.2 (2006).
15. He, Qinghua, et al. «Brain anatomy alterations associated with Social Networking Site addiction». (2017)
16. Kahneman, Daniel. «Thinking, fast and slow». Macmillan (2011)
17. Knutson, Brian, et al. «Dissociation of reward anticipation and outcome with event-related fMRI». Neuroreport 12.17 (2001)
18. Kramer, Adam DI, et al. «Experimental evidence of massive-scale emotional contagion through social networks». Proceedings of the National Academy of Sciences 111.24 (2014)
19. Martin, Dominic. «#republic: Divided Democracy in the Age of Social Media». Princeton University Press. Business Ethics Quarterly (2018)
20. Mellor, Maria. «Why Is TikTok Creating Filter Bubbles Based on Your Race?» (2020),www.wired.co.uk/article/tiktok-filter-bubbles
21. Papadamou, Kostantinos, et al. «Disturbed YouTube for kids: Characterizing and detecting inappropriate videos targeting young children». Proceedings of the international AAAI conference on web and social media. Vol. 14. (2020)
22. Pariser, Eli. «The filter bubble: How the new personalized web is changing what we read and how we think». Penguin (2011)
23. Ra, Chaelin K., et al. «Association of digital media use with subsequent symptoms of attention-deficit/hyperactivity disorder among adolescents». Jama (2018), https://jamanetwork.com/journals/jama/article-abstract/2687861
24. Santos, Fernando P., et al. «Link recommendation algorithms and dynamics of polarization in online social networks». Proceedings of the National Academy of Sciences 118.50 (2021)

25. Schmuck, Desirée. «Following Social Media Influencers in Early Adolescence: Fear of Missing Out, Social Well-Being and Supportive Communication with Parents». Journal of Computer-Mediated Communication 26.5 (2021): 245-264.
26. Schüll, Natasha Dow. «Addiction by design». Princeton University Press (2012)
27. Turel, Ofir, et al. «Health outcomes of information system use lifestyles among adolescents: videogame addiction, sleep curtailment and cardio-metabolic deficiencies». PloS one 11.5 (2016)
28. Van Deursen, Alexander JAM, et al. «Modeling habitual and addictive smartphone behavior: The role of smartphone usage types, emotional intelligence, social stress, self-regulation, age, and gender». Computers in human behavior 45 (2015): 411-420.
29. Zuiderveen Borgesius, Frederik, et al. «Should we worry about filter bubbles?» Internet Policy Review. Journal on Internet Regulation 5.1 (2016)
30. «Chamath Palihapitiya, Founder and CEO Social Capital, on Money as an Instrument of Change». Stanford Graduate School of Business (2017)
31. «Filter Bubble – A Built-In Bias in Your Social Media Feed and Searches». Aarambh Child Protection (2021), http://aarambhindia.org/filter-bubble-built-bias-social-media-feed-searches/
32. «High Amounts of Screen Time Begin as Early as Infancy, NIH Study Suggests». National Institutes of Health (2019), www.nih.gov/news-events/news-releases/high-amounts-screen-time-begin-early-infancy-nih-study-suggests
33. «Pathways: How digital design puts children at risk», 5Rights Foundation (2021), https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf
34. «The Facebook Whistleblower Says Its Algorithms Are Dangerous. Here's Why». MIT Technology Review (2021)

22. Игровая зависимость

Игровая зависимость характеризуется постоянной, повторяющейся потерей контроля над игровым процессом, повышением приоритета игр над другими интересами и повседневной деятельностью ребенка, а также продолжением или эскалацией этой модели поведения, несмотря на возникновение негативных последствий.

Статус персонажа и достижения в игре напрямую зависят от затраченного времени. При этом во многих играх есть платные внутриигровые предметы, которые дают пользователю преимущество, что оказывает сильное давление на неокрепшую психику детей и подростков.

Зависимость от игр вызывает различные проблемы с социальным, психологическим и даже физическим состоянием. Она приводит к нарушению классического социального взаимодействия ребенка с семьей и друзьями, меняет образ жизни, мешает академической успеваемости.

Специфика риска

Видеоигровая зависимость — относительно новое расстройство, поэтому на данный момент оно все еще изучается научным сообществом.

Исследователи выделяют 5 основных симптомов:

1. видеоигры становятся доминирующей деятельностью в жизни человека, когда он вкладывает в них время в ущерб другой деятельности;
2. потеря интереса к предыдущим увлечениям и другим аспектам жизни;
3. раздражение или грусть при отсутствии доступа к играм;
4. обман себя и кого-либо по поводу потраченного на игры времени;
5. человек продолжает играть, несмотря на то, что понимает возможный ущерб от этого действия.

Появление игровой зависимости обусловлено разными причинами, наиболее распространенными у детей считаются уход от реальности и повышение социального статуса. Уход от реальности — из-за различных отрицательных обстоятельств и событий в жизни ребенка он находит в игре место, где все эти проблемы забываются. Игры становятся своего рода убежищем от реальности.

Повышение социального статуса — большинство игр устроено по принципу ежедневных заданий, за выполнение которых дается вознаграждение, и других активностей, побуждающих постоянно находиться в игре. Все это дает преимущество тем игрокам, которые проводят все свое время игре, а соответственно, делает их персонажей ценнее, чем персонажи их сверстников.

Современные игры используют модель free-to-play[10] с последующей монетизацией за счет продажи внутриигровых предметов за деньги. Эти предметы дают либо какое-то преимущество в игре, либо способ выделиться среди других игроков. Подобные факторы оказывают сильное давление на неокрепшую психику подростков, и подталкиваю детей к покупке.

[10] Free-to-play — способ распространения компьютерных игр, позволяющий пользователю играть без внесения денежных средств.

Дети подвергаются проявлению синдрома упущенной выгоды, который стимулируется постоянными игровыми событиями или специальными «ограниченными» предложениями от разработчиков игр. Участие в таких событиях или приобретение подобных предметов присваивает игрокам особый статус. Все это усугубляется бесконечным потоком контента, который необходимо осваивать, чтобы поддерживать свой статус в игре — это развивает у ребенка взаимосвязь между потраченным временем на игру и развитием его персонажа, что в итоге приводит к тому, что ребенок хочет находиться в игре постоянно.

Последствия

Зависимость от игр вызывает различные проблемы с социальным, психологическим и даже физическим состоянием. Эта форма поведения человека забирает большую часть времени и сильно отражается на его жизни, она приводит к нарушению классического социального взаимодействия, меняет образ жизни, мешает академической успеваемости или работе, а также оказывает воздействие на развитие личности.

Физические последствия: длительное времяпрепровождение за играми приводит к ухудшению зрения, появлению у детей проблем с опорно-двигательной системой, болям в спине, шее, копчике и в запястьях. У человека, поглощенного игрой, нарушается режим сна и качество питания — все это приводит к избыточному весу и в крайней степени к ожирению.

Психологические последствия: нездоровое увлечение играми пагубно влияет на психику человека, в особенности на неокрепшую психику ребенка, и это может привести к последствиям различного характера. У детей, зависимых от игры, наблюдается заниженная самооценка в реальной жизни. Если они долгое время не играют, то проявляют агрессию и повышенную возбужденность или наоборот — приходят в отчаяние или грустят. У подростков с этим заболеванием чаще всего есть проблемы с социализацией в реальной жизни, им сложнее общаться с людьм. Крайняя форма последствий — потеря связи с реальностью, что может привести к смерти или суициду.

Распространенность

Так как заболевание относительно новое, ученые пока не вывели стабильные и универсальные средства диагностики. Культура страны и особенности выборки также сильно влияют на результаты исследования. Из-за этого данные по распространенности — гетерогенные.

В исследовании, проведенном в США, Великобритании, Канаде и Германии, было выявлено, что 1 % всего населения потенциально имеет зависимость от игр.

В Японии было проведено национальное исследование по игровой зависимости, в 2017 году до 27,5 % игроков имели признаки этого заболевания.

Норвежское исследование 2015 года среди любителей игр показало, что 1,4 % игроков можно было назвать зависимыми и 7,3 % — близкими к зависимости.

Исследование, проведенное в Гонконге в 2017 году, показало, что в среднем 13,9 % студентов мужского пола проводили за видеоиграми более 20 часов в неделю.

Ученые предполагают, что около 1-3 % всех людей в мире болеют зависимостью от видеоигр. Зависимость куда чаще проявляется у мужчин, чем у женщин, и людей старшего возраста

затрагивает реже, чем детей, подростков и молодых людей. У полов есть статистическая разница в предпочтениях касательно видеоигр и отношении к ним.

По данным опроса Piper Sandler, в 2019 году подростки мужского пола тратили 14 % своих денег на видеоигры. В 2021 подростки в целом тратили 8 % своих денег на видеоигры, а 52 % подростков собирались покупать новое поколение консолей, несмотря на их высокую стоимость.

Согласно годовому отчету от App Annie, за 2021 год пользователи потратили более 320 млн долларов на внутриигровые предметы, что на 20 % больше чем в 2020 году.

В 2021 году среднестатистический пользователь проводил в мобильных играх 4,8 часа в день. В итоге за 2021 год было затрачено на мобильный гейминг 3,8 триллиона часов.

Примеры

Кэмерон Адэр (2019)

История Кэмерона началась в 18 лет, когда в его жизни появились проблемы в учебе, отношениях и на работе. Он отмечал развитие депрессии и не знал, куда тратить высвобожденное время. Тогда он и нашел утешение в компьютерной игре World of Warcraft. Каждый день он просыпался с мыслью, что его ждет игра. Кэмерон тратил часы напролет, развивая своего персонажа, не обращая внимания на проблемы в реальной жизни. Игровой мир заменил ему реальный, а общение в игре заменило друзей. Добившись высоких результатов в игре, он стал частью внутриигрового общества, которое побуждало тратить еще больше времени онлайн. В конечном итоге Кэмерон заметил, что у него нет ничего, кроме игры, и все социальные связи в его жизни разорваны. Это побудило Кэмерона преодолеть зависимость, пока его жизнь не полностью вышла из под его контроля.

Кэмерон Адэр излечил свою игровую зависимость и живет полноценной жизнью. В конечном итоге он основал организацию для помощи другим людям в борьбе с зависимостью от компьютерных игр, Game Quitters.

Смерть Ким Са-Ран (2010)

Мужчина в возрасте 41 года и женщина в возрасте 25 лет решили завести ребенка. Вскоре они потеряли работу, а девочка родилась раньше срока. Пара тратила все доступное время в интернет-кафе, заглядывая домой только для того, чтобы покормить своего ребенка смесью для новорожденных. Все остальное время они играли в Prius Online — видеоигру, одной из главных особенностей которой является уход за виртуальным ребенком. Так пара завела себе второго, виртуального ребенка, и ухаживала за ним больше, чем за реальной дочерью.

В сентябре они вернулись домой после 12-часовой игровой сессии и нашли девочку мертвой. Полиция определила, что ребенок умер от голода, и решила расследовать произошедшее как преступление.

Случай с FIFA (2019)

В футбольном симуляторе FIFA у каждого спортсмена есть карточка. Если в профиле игрока есть карточка футболиста, его виртуальной копией можно пользоваться в игре. Но покупать

специальные карточки спортсменов можно только пачками — набором сразу из нескольких карточек. Такую пачку надо вскрыть, чтобы пользоваться виртуальными спортсменами. Проблема в том, что пока игрок не вскроет колоду карточек, он не знает, каких футболистов он покупает. Это один из многих примеров темных паттернов, которыми могут пользоваться корпорации в индустрии видеоигр.

Томас Картер, житель Великобритании, купил одну пачку своим 4 детям, но не учел, что дети это видели. Спустя какое-то время, его кредитная карточка дала сбой: на ней закончились деньги. Оказалось, что дети потратили 550 фунтов стерлингов на то, чтобы получить виртуального Лионеля Месси, их любимого спортсмена. Они продолжали тратить деньги, когда в очередной пачке карточек футболиста не оказывалось. Даже когда деньги на счету их отца кончились, дети все еще не получили желанного спортсмена.

Источники

1. Adair, Cam. «How to Beat Your World of Warcraft Addiction». Game Quitters (2021), gamequitters.com/world-of-warcraft-addiction
2. App, Annie. «The State of Mobile in 2022: How to Succeed in a Mobile-First World As Consumers Spend 3.8 Trillion Hours on Mobile Devices». Report (2021)
3. Ayenigbara, I. «Gaming Disorder and Effects of Gaming on Health: An Overview» (2018)
4. Blaine, R., et al. «Promoting Sleep and Balanced Screen Time among School-Aged Children with Neurodevelopmental and Mental Health Disorders: A Parent Perspective» (2021)
5. Bloemen, Noor and David De Coninck. «Social Media and Fear of Missing Out in Adolescents: The Role of Family Characteristics». Social Media and Society 6.4 (2020)
6. Coulson, Josh. «Just 26% of EA's Revenue Now Comes From Game Sales». TheGamer (2021), https://www.thegamer.com/26-ea-revenue-game-sales/.
7. Kleinman, By Zoe. «My Son Spent £3,160 in One Game». BBC News (2019), www.bbc.com/news/technology-48925623
8. Lin, C., et al. «Internet gaming disorder, psychological distress, and insomnia in adolescent students and their siblings: An actor-partner interdependence model approach» (2021)
9. Melodia, F., et al. «The Role of Avoidance Coping and Escape Motives in Problematic Online Gaming: A Systematic Literature Review» (2020)
10. Mihara, S. and S. Higuchi. «Cross-sectional and longitudinal epidemiological studies of Internet gaming disorder: A systematic review of the literature». (2015)
11. Paulus, F., et al. «Internet gaming disorder in children and adolescents: a systematic review» (2018)
12. Przybylski, A. K., et al. «Internet Gaming Disorder: Investigating the Clinical Relevance of a New Phenomenon». (2016)
13. Q. Xu, M. Zhang. «The Research on Critical Factors Affecting the Game Experience of Daily Quests System in Mobile Game». (2020)
14. Stevens, MW, et al. «Global prevalence of gaming disorder: A systematic review and meta-analysis». (2021)
15. Teng, Z., et al. «Depression and anxiety symptoms associated with internet gaming disorder before and during the COVID-19 pandemic: A longitudinal study». (2021)
16. Vidua, R., et al. «Suicide linked to PUBG video gaming: A case report». (2020)
17. Wittek, C., et al. «Prevalence and Predictors of Video Game Addiction: A Study Based on a National Representative Sample of Gamers» (2016)
18. Zamani, E., et al. «Effect of Addiction to Computer Games on Physical and Mental Health of Female and Male Students of Guidance School in City of Isfahan» (2009)
19. «37th Semi-Annual Taking Stock With Teens Survey». Piper Sandler (2021)
20. «Campaign for a Commercial-Free Childhood». Center for Digital Democracy (2021)

21. «Diagnostic and Statistical Manual of Mental Disorders. 5th edn». American Psychiatric Association (2013)
22. «Girl starved to death while parents raised virtual child in online game». The Guardian (2010), https://www.theguardian.com/world/2010/mar/05/korean-girl-starved-online-game
23. «International Classification of Diseases-11». WHO (2018)
24. «Survey on the Gaming Habits among Hong Kong Upper Primary Students: major findings and conclusion». The University of Hong Kong (2017)
25. «The kids emptied our bank account playing Fifa». BBC (2019), https://www.bbc.com/news/technology-48908766

23. Избыточное использование интернета

Избыточное использование интернета приводит к нарушению психологического, социального, личностного, академического или профессионального благосостояния человека.

К основным симптомам интернет-зависимости относится не только увеличение количества времени, проведенного в интернете, но и перепады настроения, чувство одиночества, беспокойство и раздражительность.

Например, фильтры, инструменты для ретуши и обработки фотографий формируют у детей и подростков неверные представления о внешности, что приводит к комплексам в реальной жизни.

Специфика риска

К основным симптомам интернет-зависимости относится не только увеличение количества времени, проведенного в интернете, но и перепады настроения, включая чувство одиночества, беспокойство и раздражительность. Помимо этого, интернет-зависимые склонны отказываться от ответственности и отрицать проблемы, что способствует переходу из реального мира в виртуальный. Зависимые от интернета подростки чаще всего не могут контролировать время, проведенное онлайн, а также не в состоянии сократить его самостоятельно.

Причинами могут являться недостаточное внимание родителей, неуверенность в себе и застенчивость, недостаток общения со сверстниками и значимыми людьми, комплексы и трудности в общении, отсутствие других увлечений и хобби, любых привязанностей.

Для подростков интернет-пространство обладает характеристиками, неосознанно привлекающими их внимание. Интернет создает иллюзию вседозволенности и безнаказанности, дает возможность самореализации, способствует удовлетворению коммуникативных потребностей, помогает установить принадлежность к группе по интересам, предоставляет бесконечный поток новой информации, игр и развлечений.

Дети, которые проводят большую часть своего времени в виртуальном мире, становятся зависимыми от интернета и начинают чувствовать себя оптимистичными, принятыми и услышанными только в онлайн-среде. А в случаях, когда они не могут получить доступ к интернету, начинают испытывать беспокойство, печаль и депрессию.

Интернет можно использовать для множества полезных задач, однако интернет-зависимые тратят большую часть своего времени на просмотр ленты в социальных сетях и компьютерные игры. Они не могут отслеживать время, которое тратят на это, в результате чего могут стать менее продуктивными. Так, по данным исследования, около 70 % опрошенных подростков и студентов считают, что их успеваемость снизилась из-за того, что они долго находятся в интернете.

Большинство подростков заходят в интернет перед сном, при этом некоторые из них продолжают просматривать контент в течение долгих часов. В результате они страдают от проблем, связанных со сном.

Учеными также была выявлена высокая корреляция между социальной изоляцией и интернет-зависимостью. Те, кто проводит много времени в интернете, как правило, становятся

частью одного или нескольких онлайн-сообществ. В конечном итоге у них развиваются тесные дружеские отношения. Чтобы оставаться на связи с друзьями в интернете, подростки проводят в сети по несколько часов в день и часто чувствуют себя оторванными от семьи и сверстников.

У зависимых от интернета подростков наблюдается дисморфофобия — это психическое расстройство, при котором человек чрезмерно обеспокоен и занят незначительным дефектом или особенностью своего тела. В опросе, проведенном британским Фондом психического здоровья, 40 % молодых людей заявили, что изображения в социальных сетях заставили их беспокоиться об имидже своего тела. Опрос Dove Detoxify 2021 года показал, что 67 % канадских девочек пытаются изменить или скрыть хотя бы одну часть тела, прежде чем публиковать свою фотографию. А к 13 годам большинство (80 %) девочек уже применяли фильтр или использовали приложение для ретуши, чтобы изменить внешний вид на фотографиях.

Результаты анализа 2018 года показали значительно больший уровень распространенности суицидальных мыслей из-за интернет-зависимости у молодежи в возрасте до 18 лет по сравнению с показателем, наблюдаемым у взрослых. Исследования, включенные в этот метаанализ, также свидетельствуют, что у подростков был самый высокий уровень распространенности интернет-зависимости (18,7 %).

Боль в спине и шее, а также головные боли являются распространенными последствиями, связанными с избыточным использованием компьютера. Помимо этого, фокусировка глаз на одной и той же точке в течение длительного времени вызывает усталость. Подсветка экрана также может вызвать усталость глаз. Хотя нет никаких доказательств того, что усталость глаз снижает зрение, пользователи могут столкнуться с помутнением зрения, временной неспособностью сосредоточиться на далеких объектах и головными болями.

Распространенность

По данным исследования, интернет-зависимости подвержены более 40 % подростков. В России самыми зависимыми от интернета являются подростки в возрасте от 14 до 17 лет, их число составляет 75,5 % всех опрошенных (всего опрошено 3,3 млн подростков).

Из-за мер, связанных с распространением COVID-19, дети стали проводить в интернете больше времени. Более половины (53 %) родителей не говорили со своими детьми об увеличении времени в интернете во время локдауна, а треть (29 %) не думали, что такие разговоры изменят ситуацию.

Исследование Digital Wellbeing 2020 показывает, что половина подростков (52 %) признаются, что они стали зависимы от смартфонов. Также 42 % подростков отмечают, что их родители аналогично зависимы. Большинство респондентов чувствовали, что их связь с технологиями негативно повлияла на их жизнь.

По результатам опроса 120 детей в возрасте от 9 до 11 лет, большинство детей (72,7 % мальчиков и 44,5 % девочек) сообщили, что если дома компьютер занят, они проводят время в играх на планшете или телефоне. 33,4 % мальчиков и 18,6 % девочек отметили, что не могут найти интересное занятие в случае, когда компьютер занят или сломан. При этом 12,4 % девочек и 22,1 % мальчиков испытывают раздражение, если им запрещают проводить время за компьютером.

Более 85 % российских студентов систематически пренебрегают сном ради того, чтобы подольше посидеть в интернете, а 76 % пренебрегают домашними делами. Более 50 % предпочитают пребывание в сети живому общению. При этом по данным другого исследования выяснилось, что 67 % участников сообщили об ухудшении самочувствия из-за социальных сетей.

Чем больше времени дети проводят перед экраном, тем больше риск развития болей в шее или спине уже в возрасте 11-12 лет. Дети, которые ежедневно проводят не менее 6 часов в телефоне и за компьютером, имели в два-три раза больший риск сильной боли в спине по сравнению с детьми, у которых экранное время составляло менее 2 часов.

Согласно результатам опроса, 29,4 % мальчиков в возрасте 9-11 лет чувствуют себя хорошо, проводя время за компьютером. Каждый пятый (21,3 %) отметил, что иногда чувствует боль в глазах. О болях в спине и шее из-за продолжительного использования компьютера упомянули 18,7 % мальчиков. Девочки от 9 до 11 лет прежде всего отметили боль в глазах (23,9 %), боль в спине и шее отмечали 22,8 % девочек, а 16,9 % сказали, что испытывают головную боль или головокружение.

Примеры

Интернет-зависимость привела к депрессии (2017)

Когда 14-летнему юноше из Индии подарили ноутбук, он пользовался интернетом по необходимости — не более 15 минут в день. Постепенно он начал пользоваться интернетом в течение 4-6 часов в день, это время уходило на игры и социальные сети. По словам юноши, он не мог контролировать время своего пребывания в интернете. Даже в школе он думал о подключении к интернету и чувствовал тревогу без доступа к сети. Затем юноша начал проводить время в интернете до поздней ночи: помимо ленты в соцсетях, смотрел порнографию.

Мальчик показал плохие результаты на экзаменах, его успеваемость резко снизилась. Спустя 6 месяцев юноша стал быстро уставать, перестал общаться с семьей и друзьями. У него пропал аппетит, вследствие чего он похудел и выглядел истощенным. Он все чаще говорил о безнадежности, пребывал в депрессивном состоянии и даже выражал желания умереть.

Психические расстройства и агрессия из-за компьютерных игр (2015)

17-летний мальчик, который входил в тройку лучших учеников до восьмого класса, начал играть в онлайн-видеоигры в девятом классе. Впоследствии он стал проводить за компьютером по 10-14 часов в день, пропускал занятия и не сдавал экзамены. Он перестал ходить в школу и не общался с окружающими.

Со временем юноша стал проявлять агрессию — несколько раз поднимал руку на свою мать. Из-за чрезмерной активности в интернете у него развились боли в шее, усталость и напряжение глаз. У него были выявлены психические расстройства, связанные с чрезмерным использованием интернета и компьютерных игр.

Зависимость от интернета у тринадцатилетней девочки (2016)

Девочка в возрасте 13 лет чувствовала себя одинокой и никому не нужной. В ее семье наблюдались частые конфликты. Она нашла «поддержку» на сайте знакомств, куда выкладывала свои обнаженные фото.

Девочка ушла из дома, когда родители попытались пресечь ее увлечение интернетом. Она бродяжничала и воровала для того, чтобы пополнить счет на телефоне и оставаться онлайн.

Зависимость от социальных сетей (2019)

16-летняя девочка пристрастилась к социальной сети Instagram*. Однажды она с родителями уехала из дома, но забыла свой телефон. Из-за этого девушка расплакалась и начала паниковать, потому что не сможет зайти в социальную сеть целый час. По словам матери, она не выпускает телефон из рук — ужинает, смотрит телевизор и ходит в ванную комнату только с ним.

Все попытки родителей забрать телефон у девочки или поговорить о том, что она слишком много времени уделяет социальным сетям, приводят к тому, что подросток пугается и проявляет агрессию.

Источники

1. Бильгин Мехмет. «Исследование особенностей интернет-зависимости у подростков». Психология. Историко-критические обзоры и современные исследования 7.6A (2018): 175-186
2. Дувалина О. Н. и Е. А. Чернявская. «Феномен интернет-аддикции как одна из причин девиантного поведения подростков». Colloquium-journal. No. 6 (30). Голопристанський міськрайонний центр зайнятості (2019)
3. Кочиобан Алина. «Негативное влияние компьютера и интернета на психику и физическое здоровье детей». International Academy Journal Web of Scholar № 1 (43) (2020)
4. Мылтасова О. В. и А. А. Овсянникова. «Интернет-зависимость и влияние онлайн-игр на подростков». Современное общество: вопросы теории, методологии, методы социальных исследований (2019)
5. Николаева Эльвира и Светлана Румянцева. «Интернет-зависимость подростков как информационно-психологическая угроза». Балканско научно обозрение 3.1 (3) (2019).
6. Скобликова Т. В. и Е. В. Скриплева. «Интернет-зависимость в молодежной среде как одна из проблем современного общества». Современные проблемы науки и образования №2 (2020)
7. Соловьева Е.Н. «Интернет-зависимость в практике детского психотерапевта». Научное обозрение. Медицинские науки № 4 (2016)
8. Юрченко О. В. и Н. Ф. Дианова. «Проблема интернет зависимости у подростка». Вестник современных исследований 12.8 (2018)
9. Cheng, Yu-Shian, et al. «Internet addiction and its relationship with suicidal behaviors: a meta-analysis of multinational observational studies». The Journal of clinical psychiatry 79.4 (2018)
10. Joergensen, Anne Cathrine, et al. «Spinal pain in pre-adolescence and the relation with screen time and physical activity behavior». BMC musculoskeletal disorders 22.1 (2021)
11. Mamidipalli, S.S., et al. «Report of Internet Addiction from Indian subcontinent: Diverse in geography but similar in form». Psychol Behav Sci Int J (2017)
12. Sharma, Manoj Kumar and Poornima Mahindru. «Video game addiction: Impact on teenagers' lifestyle». Natl Med J India (2015)
13. Yuvaraj, T. and Dr. Suresh A. «A review on the definitions of internet overuse behavior».(2018)
14. «Body Image in Childhood». Mental Health Foundation (2020)

15. «Digital Wellbeing 2020». The Cybersmile Foundation (2021)
16. «Dove Detoxify Survey». Dove (2021)
17. «Half of Children and Teens Exposed to Harmful Online Content While in Lockdown». BBFC (2020), https://www.bbfc.co.uk/about-us/news/half-of-children-and-teens-exposed-to-harmful-online-content-while-in-lockdown
18. «How Media Use Can Affect Kids (for Parents) — Nemours KidsHealth». KidsHealth (2021), kidshealth.org/en/parents/tv-affects-child.html
19. «Internet Overuse and Addiction». The University of Melbourne, services.unimelb.edu.au/counsel/resources/addictive-behaviours/internet-overuse-and-addiction
20. «My Teenage Daughter's Social Media Use Has Become Really Obsessive». The Irish Times (2019)

Технологические решения по защите детей в интернете

Для того чтобы определить спектр существующих технологических решений, направленных на обеспечение безопасности детей в интернете, мы проанализировали более 300 патентов, компаний и ИТ-решений в этой области. По результатам анализа было сформировано 8 кластеров технологических решений:

1. Предиктивная аналитика
2. Детские социальные сети
3. Практики разработки
4. Инструменты родительского контроля и мониторинга
5. Интернет-фильтры
6. Автоматизированная модерация
7. Сервисы оказания помощи
8. Инфраструктура

1. Предиктивная аналитика

Предиктивная аналитика — это статистические и аналитические инструменты, которые используются для прогнозирования будущих событий или поведения.

Предиктивные системы используют большие данные, статистику, а также искусственный интеллект и машинное обучение. Предиктивная аналитика может использоваться для моделирования среды, прогнозирования и раннего выявления рисков различного характера. На предиктивных моделях базируется анализ пользовательского поведения онлайн и предиктивная криминология в киберпространстве.

Предиктивная аналитика позволяет изучать и классифицировать источники риска и ранжировать их в соответствии с возрастными группами детей. Основная задача — это раннее выявление источников риска по определенным признакам с помощью алгоритмов.

К основным методам предиктивной аналитики, направленным на обеспечение защиту детей в интернете, относят изучение онлайн-среды, профилирование и анализ графа связей.

Изучение онлайн-среды — анализ алгоритмов, устройств, пользовательских привычек детей, их интернет-взаимодействий с учителями и родителями и многое другое. Исследования проводятся для определения и прогнозирования того, каким образом дети могут столкнуться с рисками, а также для выявления ключевых факторов, способствующих уязвимости ребенка к этим рискам. Например, такие системы используются в борьбе с кибербуллингом.

Профилирование — длительное наблюдение и сбор данных о ребенке из различных источников, например, паттерны пользования смартфоном, лингвистический анализ сообщений в мессенджерах, постов и комментариев в соцсетях, анализ аудиосообщений, модуляции голоса, интенсивности общения, а также других данных из приложений. Помимо этого, данные могут собираться с умных устройств. Это позволяет вычислять уязвимость к рискам, включая наличие психологических травм, отклонений, заболеваний. Так можно предсказать поведение ребенка, а также конкретные опасности, которые для него представляет окружающее офлайн- и онлайн-пространство. Поведение жертвы является важным компонентом преступления, поэтому часть систем строится именно на анализе поступков детей.

Профилирование применимо не только по отношению к жертвам: существуют паттерны в поведении преступников, которые заинтересованы в жертвах-детях. Поиск таких паттернов и дальнейшее наблюдение за подозреваемыми позволяют понять, насколько человек может быть опасен для ребенка, и предотвратить преступление. Во многих случаях такие системы строятся на данных, накопленных у правоохранительных органов. Более того, лингвистические модели позволяют понять, насколько преступник склонен к рецидивам.

Анализ графа связей — это выявление всех связей пользователя в различных социальных сетях, мессенджерах и телефонных контактах. С помощью анализа связей можно определить частые интенсивные контакты взрослых людей и несовершеннолетних, а также обнаружить преступные группировки, например, активистов групп смерти или иные деструктивные движения. Это позволяет заблаговременно запустить мониторинг за детьми, в чьих кругах присутствуют лица, склонные к определенным рискам или уже столкнувшиеся с ними.

В ходе анализа данных формируются артефакты, которые позволяют строить прогнозы на основании выявленных ранее закономерностей. Цифровые следы пользователя, накопившиеся за длительный промежуток времени, составляют цифровую ДНК пользователя. Маркеры — это индикаторы, элементы данных в цифровой ДНК, совпадающие с заданными свойствами, по

которым составляются прогнозы. Предикторы представляют собой определенные явные признаки в паттерне поведения, являющиеся сигналом возможного риска. Поскольку изначально определяются стадии развития риска, то и предикторы для каждой стадии будут разные. Наличие предикторов из нескольких категорий и стадий подтверждают большую вероятность наступления риска.

Уровень уязвимости детей к онлайн-рискам зависит от множества факторов:

- доступность ребенка в интернете для мотивированных преступников — онлайн-поведение, способствующее повышению вероятности прямого столкновения с рисками;
- отсутствие защиты — отсутствие технологических средств защиты или контакта с родителями;
- некорректное поведение — непонимание ребенком онлайн-рисков, неподготовленность, рискованное и провоцирующее поведение.

Благодаря предиктивной аналитике можно определить и спрогнозировать поведение ребенка, возможные угрозы и риски, с которыми он может столкнуться. Предиктивная аналитика также позволяет отслеживать психологическое состояние ребенка**.** Оно определяется через длительное наблюдение со сбором различных данных. Например, лингвистический анализ из различных источников и тональность голоса при общении могут определять и прогнозировать депрессию и уровень стресса у детей.

Алгоритмы нейросетей могут определять риск суицидальных настроений через тексты постов и фотографии в различных социальных сетях, например, в Instagram* и Twitter. Среди учащихся проводятся исследования и сбор данных для алгоритмов машинного обучения, которые смогут выявлять в ранней стадии склонность к суицидальному поведению , определять текущую депрессию и проблемы с самооценкой.

В предиктивных моделях также используются данные о «стилях родительства», собранные из приложений родительского контроля и мессенджеров.

Современные предиктивные методы уже достаточно продвинулись в том, чтобы определять самые ранние маркеры и предикторы, указывающие на высокую вероятность развитие зависимости к интернету и смартфонам у детей.

Помимо этого, программы и приложения, работающие в школах, могут быть использованы для прогнозирования успехов в учебе. Алгоритмы могут выявлять паттерны поведения в учебном процессе, например, пропуски и посещения, а также некоторые признаки, которые могут указывать на проблемы ребенка в семье или в отношениях со сверстниками.

Ограничения

Применение предиктивной аналитики связано с техническими и этическими ограничениями**.**

Технические ограничения

Точность прогнозов напрямую связана с количеством и качеством данных, которые используются для машинного обучения. В некоторых случаях для обеспечения эффективности прогнозирования требуются данные, собранные более чем с миллиона наблюдений. При этом

сбор данных и машинное обучение требуют большого количества времени и постоянной проверки модели. Разработка итоговой версии алгоритма может занимать несколько лет.

Системы предиктивной аналитики принимают решения на основе данных, полученных из среды. Но в некоторых случаях, когда решения системы начинают влиять на среду, производя заведомо корректный материал для обработки, появляются петли обратной связи. В итоге получается кибернетический аналог радикализации, когда система разгоняется в одну сторону, повторяя решения в одном и том же направлении. Одной из причин такого самоповтора является узкая направленность разрабатываемых ИИ-решений. Это может повлечь за собой необоснованные обвинения в преступной деятельности или неверные прогнозы по поводу психологического здоровья ребенка.

Этические ограничения

Предиктивная аналитика и профилирование влекут за собой ряд этических и правовых вопросов, например, связанных с защитой персональных данных детей.

В зарубежной литературе активно обсуждается проблема дискриминации искусственным интеллектом отдельных этнических групп. Это связано с тем, что алгоритмам предоставляются сырые данные, например, статистика ФБР. Такие данные не всегда включают в себя контекст о причинах в статистической разнице криминализации разных этнических групп. Учитывая, что на данный момент ИИ не способен самостоятельно осознавать контекст, это приводит к ложным тревогам, которые могут оказать существенный негативный эффект на жизнь человека.

Примеры

LearningCurve

LearningCurve — программа обработки больших данных из образовательных учреждений с предиктивной аналитикой. На базе этих данных и машинного обучения компания Pearson разрабатывает модель для повышения эффективности образования. Однако аналитика используется не только для управления образовательными процессами, но и для профилирования учеников. Благодаря этому создаются прогнозы, касающиеся успеваемости, поведения, ментального здоровья и рисков развития ребенка, создаются профили учителей и анализируется их модель взаимодействия с учениками.

TripleP

TripleP — организация, которая занимается проведением тренингов для родителей и использует предиктивную аналитику. При прохождении программы тренировок организация собирает данные о родителях и детях. Эти базы данных используются для обучения ИИ и дальнейшего использования предиктивной аналитики. Так организация получает точные профили родителей и детей, выявляет проблемы в семье и получает углубленное понимание развития каждого ребенка.

Алгоритм для предотвращения суицидов

Алгоритм создан университетом Бригама Янга в кооперации с Гарвардом. Ученые нашли главные предикторы, которые диктуют подростковую тенденцию к суициду. С помощью машинного обучения и больших данных алгоритм способен определять, насколько подросток склонен к суицидальному поведению, мыслям об этом и самому самоубийству. Точность прогнозирования составляет 91 %, а база данных, по которой обучался алгоритм, основана на

результатах опроса более 175 тысяч учеников. Алгоритм разработан профессорами Майклом Барнсом и Карлом Хэнсоном из университета Бригама Янга (США, Юта).

PrevBOT

PrevBOT — чат-бот, базирующийся на алгоритмах, предназначенный для помощи полиции в выявлении злоумышленников в чатах, мессенджерах и социальных сетях. Бот может работать в режиме наблюдателя, который фиксирует чужие переписки, а также в режиме имитации ребенка, заточенной на привлечение злоумышленников. Лингвистическая модель робота позволяет определять пол, возраст и авторский почерк человека и соотносить его с базой киберпрофилированных аккаунтов других потенциальных преступников. Так можно выявить одного злоумышленника, который ведет несколько аккаунтов в одной соцсети или аккаунты в разных соцсетях. Кроме того, так как бот способен распознавать преступников и определять, какие цифровые пространства они оккупируют, его можно использовать как инструмент для определения опасных для детей сообществ.

Источники

1. Al-Garadi, Mohammed Ali, et al. «Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithms: Review of Literature and Open Challenges». IEEE Access vol. 7 (2019)
2. Asniar and Kridanto Surendro. «Predictive Analytics for Predicting Customer Behavior». International Conference of Artificial Intelligence and Information Technology (2019)
3. Azcona, David, et al. «Detecting students-at-risk in computer programming classes with learning analytics from students' digital footprints» (2019)
4. Babchishin, Kelly M., et al. «Online Child Pornography Offenders are Different: A Meta-analysis of the Characteristics of Online and Offline Sex Offenders Against Children» (2015)
5. Bin Morshed, Mehrab, et al. «Measuring Self-Esteem with Passive Sensing» (2020)
6. Burnap, Pete, et al. «Multi-class machine classification of suicide-related communication on Twitter». Online social networks and media 2 (2017)
7. Calderoni, Francesco. «Social Network Analysis of Organized Criminal Groups. Encyclopedia of Criminology and Criminal Justice» (2014)
8. Clark, Lynn Schofield. «The Parent App: Understanding Families in the Digital Age». European Journal of Communication (2013)
9. Dogan, Huseyin, et al. «Perceived Parenting Styles as Predictor of Internet Addiction in Adolescence». International Journal of Research in Education and Science (2015)
10. Drake, Brett, et al. «A Practical Framework for Considering the Use of Predictive Risk Modeling in Child Welfare». The ANNALS of the American Academy of Political and Social Science, vol. 692, no.1 (2020)
11. Drouin, Michelle, et al. «Predicting Recidivism Among Internet Child Sex Sting Offenders Using Psychological Language Analysis». Cyberpsychol Behav Soc Netw (2018)
12. Ehrenberg, Alexandra, et al. «Personality and self esteem as predictors of young people's technology use». CyberPsychology, & Behavior, 11 (2008)
13. Ensign, Danielle, et al. «Runaway feedback loops in predictive policing». Conference on Fairness, Accountability and Transparency (2018)
14. Farsi, Maryam, et al. «Crime Data Mining, Threat Analysis and Prediction». Jahankhani H. (eds) Cyber Criminology. Advanced Sciences and Technologies for Security Applications (2018)
15. Frison, Eline and Steven Eggermont. «Browsing, posting, and liking on Instagram: The reciprocal relationships between different types of Instagram use and adolescents' depressed mood». Cyberpsychology, Behavior, and Social Networking 20.10 (2017)

16. Heilweil, Rebecca. «Algorithms and Bias, Explained». Vox (2020), www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency
17. Heirman, Wannes and Michel Walrave. «Predicting adolescent perpetration in cyberbullying: An application of the theory of planned behavior». Psicothema 24.4 (2012)
18. Hermida, Martin and Sara Signer. «How parents accompany their children on the Internet» (2013)
19. Hermida, Martin. «Schweizer Kinder und Jugendliche im Internet: Risikoerfahrungen und Umgang mit Risiken». EU Kids Online: Schweiz (2013)
20. Hernández, Montserrat Peris, et al. «The risk of sexual-erotic online behavior in adolescents – Which personality factors predict sexting and grooming victimization?» Computers in Human Behavior, Volume 114 (2021)
21. Hollingshead, Todd. «BYU algorithm accurately predicts when teens likely to have suicidal thoughts, behavior». BYU (2021), https://news.byu.edu/intellect/byu-algorithm-accurately-predicts-when-teens-likely-to-have-suicidal-thoughts-behavior
22. Kim, Bomi, et al. «The relationship between mother's smartphone addiction and children's smartphone usage». Psychiatry Investigation 18.2 (2021)
23. Kim, Ho-Kyung and Keith E. Davis. «Toward a comprehensive theory of problematic Internet use: Evaluating the role of self-esteem, anxiety, flow, and the self-rated importance of Internet activities». Computers in Human Behavior (2009)
24. Kondo, Nobuhiko, et al. «Early Detection of At-Risk Students Using Machine Learning Based on LMS Log Data». 6th IIAI International Congress on Advanced Applied Informatics (2017)
25. Ladd, Gary W. «Peer Rejection, Aggressive or Withdrawn Behavior, and Psychological Maladjustment from Ages 5 to 12: An Examination of Four Predictive Models» (2006)
26. Larsen, Mark Erik, et al. «A systematic assessment of smartphone tools for suicide prevention». PloS one 11.4 (2016)
27. Lupton, Deborah. «Digital Bodies» (2015)
28. Marciano, Laura and Anne-Linda Camerini. «Duration, frequency, and time distortion: Which is the best predictor of problematic smartphone use in adolescents? A trace data study». PloS (2022)
29. Matteini Palmerini, Riccardo. «Graph theoretical approach to sexual predator detection».NTNU (2021)
30. McCauley, Denis. «The learning curve: lessons in country performance in education». London: Pearson (2012)
31. McDaniel, Brandon. «Passive sensing of mobile media use in children and families: a brief commentary on the promises and pitfalls». Pediatric Research (2019)
32. Miró-Llinares, Fernando. «That Cyber Routine, That Cyber Victimization: Profiling Victims of Cybercrime» (2015)
33. Munro, Eileen. «Predictive analytics in child protection» (2019)
34. Nyce, Charles. «Predictive analytics white paper». American Institute for CPCU. Insurance Institute of America (2007)
35. Ongsulee, Parlwat, et al. «Big Data, Predictive Analytics and Machine Learning». 16th International Conference on ICT and Knowledge Engineering (2018)
36. Ophir, Yaakov, et al. «Deep neural networks detect suicide risk from textual facebook posts». Scientific Reports (2020)
37. Rahman, Zara and Julia Keseru. «Predictive Analytics for Children: An assessment of ethical considerations, risks, and benefits». UNICEF Innocenti Research (2021)
38. Reece, Andrew G. and Christopher M. Danforth. «Instagram photos reveal predictive markers of depression». EPJ Data Science 6.1 (2017)
39. Scharenbroch, Chris, et al. «Principles for Predictive Analytics in Child Welfare». Children Research Center (2017)
40. Sciences and Technologies for Security Applications (2018)

41. Sequeira, Lydia, et al. «Mobile and wearable technology for monitoring depressive symptoms in children and adolescents: A scoping review». Journal of Affective Disorders, Volume 265 (2020)
42. Slavich, George, et al. «Stress measurement using speech: Recent advancements, validation issues, and ethical and privacy considerations» (2019)
43. Smahel, David, et al. «EU Kids Online 2020. Survey results from 19 countries»
44. Song, Juyoung, et al. «Social Big Data Analysis of Future Signals for Bullying in South Korea: Application of General Strain Theory». Telematics and Informatics (2020)
45. Spathis, Dimitris, et al. «Passive mobile sensing and psychological traits for large scale mood prediction» (2019)
46. Stachl, Clemens, et al. «Predicting personality from patterns of behavior collected with smartphones». Proceedings of the National Academy of Sciences 117.30 (2020)
47. Staksrud, Elisabeth, et al. «What Do We Know About Children's Use of Online Technologies? A Report on Data Availability and Research Gaps in Europe» (2007)
48. Stoilova, Mariya and Sonia Livingstone. «The 4Cs: Classifying online risk to children» (2021)
49. Sunde, Nina and Inger Marie Sunde. «Conceptualizing an AI-based Police Robot for Preventing Online Child Sexual Exploitation and Abuse». Nordic Journal of Studies in Policing (2021)
50. Tanner, Lindsey. «Detecting depression: Smartphone apps could monitor teen angst». The Denver Post (2019), www.denverpost.com/2019/01/14/apps-detect-teenage-depression-angst/
51. Torous, John, et al. «Smartphones, Sensors, and Machine Learning to Advance Real-Time Prediction and Interventions for Suicide Prevention: a Review of Current Progress and Next Steps». Curr Psychiatry Rep 20, 51 (2018)
52. Weller, Orion, et al. «Predicting suicidal thoughts and behavior among adolescents using the risk and protective factor framework: A large-scale machine learning approach» (2021)
53. Whang, Leo Sang-Min, et al. «Internet Over-Users' Psychological Profiles: A Behavior Sampling Analysis on Internet Addiction». CyberPsychology & Behavior (2003)
54. Williamson, Ben. «Digital education governance: data visualization, predictive analytics, and "real-time" policy instruments». Journal of education policy 31.2 (2016)
55. Xiuqin, Huang, et al. «Mental health, personality, and parental rearing styles of adolescents with Internet addiction disorder». Cyberpsychology, Behavior and Social Networking 13 (2010)
56. Zhitomirsky-Geffet, Maayan and Maya Blau. «Cross-generational analysis of predictive factors of addictive behavior in smartphone usage». Comput. Hum. Behav. 64 (2016)
57. Zilli, Arturo. «Could Social Network Analysis Be a Useful Tool to Disarticulate Criminal Networks?» Academia (2021)
58. «Algorithmic Bias: Why And How Do Computers Make Unfair Decisions?» LibertiesEU (2021), www.liberties.eu/en/stories/algorithmic-bias-17052021/43528
59. «Teaching presence». Pearson Education (2016)

2. Детские социальные сети

Социальные сети — неотъемлемый ежедневный атрибут практически каждого современного человека, и дети не исключение. По данным BBC, более 75 % опрошенных детей используют как минимум одну социальную сеть.

Однако большинство социальных сетей, например, Twitter, Facebook* и Instagram*, не всегда безопасны для детей — используя их, ребенок может столкнуться с кибербуллингом, грумингом, секстингом[11], порнографическим контентом, а также с контентом, содержащим рекламу наркотических и алкогольных продуктов и т. д.

Решением этой проблемы могут послужить альтернативные социальные сети, созданные специально для детей. Они предлагают юным пользователям удобные функции и различные развивающие игры и приложения, а главное — обеспечивают защиту от различных интернет-угроз.

Необходимость существования социальных сетей для детей обусловлена наличием определенных рисков, с которыми несовершеннолетние могут столкнуться при использовании общих социальных платформ. Например, контент, загруженный или отправленный ребенком в социальной сети, может быть распространен без ведома и согласия отправителя. Также в обычных социальных сетях высока вероятность столкновения с ненадлежащим или деструктивным поведением со стороны пользователей. Подобный контакт может привести к кибербуллингу, секстингу и онлайн-преследованию.

Функционал социальных сетей для детей, на первый взгляд, схож с функционалом большинства обычных социальных сетей. Новостная лента, возможность общаться в личных сообщениях или создавать чаты для друзей и знакомых, выкладывать фотографии и ставить лайки. Однако разница есть, и заключается она в дополнительной безопасности пользователей и особых требованиях к контенту. Также детские социальные сети отличаются наличием образовательных и развлекательных разделов, например, с мини-играми или обучающими играми и детским видеоконтентом.

Чтобы избежать появления неподобающего и опасного контента, необходима фильтрация. Проверка каждой публикации вручную требует много времени, при этом социальные сети нуждаются в постоянном обновлении актуального контента. Поэтому большинство детских социальных сетей используют фильтры, которые автоматически блокируют публикации, содержащие грубую, ненормативную лексику или другой нежелательный тип контента. Однако подобный способ не является совершенным, и злоумышленники могут обойти систему фильтрации.

Некоторые детские социальные сети используют частичную предварительную модерацию. Когда ребенок начинает набирать фразу, алгоритм предлагает ему варианты, и если ребенок использует слово, которое неизвестно системе, публикация переходит в фазу предварительной модерации. Таким образом, часть сообщений проходят предварительную проверку, что снижает нагрузку на модераторов.

Анонимность или идентификация личности

Люди часто публикуют в соцсетях свои фотографии, дату рождения и даже адрес проживания. Этой информацией могут воспользоваться злоумышленники и грумеры. Проблема присутствия

[11] Секстинг — переписка, содержащая текст, фото или другие материалы сексуального характера.

злоумышленников в детских социальных сетях решается различными способами: одни соцсети подразумевают полную анонимность пользователей, а другие требуют идентификации при регистрации.

Предшественниками социальных сетей для детей были развлекательные порталы, где дети создавали своих цифровых персонажей, которые жили в виртуальном мире. Анонимность детей делала такие социальные сети более безопасными, но противоречила основной цели социальной сети — поддержанию связи с друзьями и сверстниками.

Альтернативой анонимности было подтверждение личности пользователя при регистрации на основе идентификатора, например, через запрос на подтверждение личности в учебное заведение или распознавание биометрии по фотографиям, сделанным веб-камерой во время регистрации. Такие методы позволяли детским социальным сетям предложить пользовательский опыт, максимально схожий с универсальными социальными сетями: ребенок создает личный профиль и может общаться со всеми друзьями, которых одобряют его родители.

В последние годы мы наблюдаем значительный рост числа пользователей социальных сетей младшего возраста. Так, более 50 % детей в возрасте от 5 до 15 лет использовали сайты или приложения социальных сетей в 2020 году. Что примечательно, более 40 % опрошенных детей использовали социальные сети до достижения минимально допустимого возраста, причем лишь малая часть получала разрешение родителей.

Ограничения

Американский закон о защите конфиденциальности детей в интернете (COPPA) запрещает любым организациям или лицам, работающим с онлайн-сервисами (включая услуги социальных сетей), собирать личную информацию лиц моложе 13 лет без разрешения родителей.

Однако дети старше 10 лет с высокой долей вероятности не захотят использовать платформу, предназначенную для детей младшего возраста. Хорошо продуманные детские приложения, которые ставят конфиденциальность на первое место и имеют строгие правила для защиты детей, нравятся родителям, но не всегда удовлетворяют целевых пользователей.

Согласно исследованиям ученых, многим детям не нравятся системы контроля, используемые на различных платформах, которые информируют родителей о выявленном нарушении в общении ребенка. Часть детей полагает, что системы автоматической проверки чатов могут совершать ошибки и обнаруживать риск для ребенка там, где его нет. Так как родители будут уведомлены об этом, и приватность диалога, которую хотел сохранить ребенок, будет нарушена. Многие дети предпочтут версии приложений и социальных сетей для взрослых, без контроля и ограничений.

Примеры

GromSocial

GromSocial — детская социальная сеть, которая учит детей укреплять уверенность и не принимать близко к сердцу злые комментарии. В GromSocial для регистрации нужно участие родителей, что позволяет свести к минимуму присутствие в ней взрослых злоумышленников.

Как только социальная сеть активируется, к ребенку в друзья попадают 17 мультипликационных персонажей, за которыми стоят модераторы, готовые помочь по любым вопросам.

Если ребенок публикует неоднозначное сообщение в интернете, или за ним замечено поведение, которое может быть спорным, сотрудники скрывают этот пост, а затем произошедшее обсуждается с виртуальным персонажем в чате.

PopJam

PopJam — это социальная платформа, объединяющая создателей контента и аудиторию в возрасте от 7 до 12 лет.

Поскольку приложение предназначено для детей, и их безопасность является ключевым вопросом, существуют определенные ограничения — дети не могут общаться с помощью приватных чатов, а также загружать фотографии, которые могут раскрыть личную информацию о них и других людях. Время публикации в приложении также ограничено с 6 утра до 11 вечера, чтобы дети могли отдохнуть.

Приложение совместимо с COPPA и Общим регламентом по защите данных Европейского Союза (GDPR). В PopJam работают модераторы, которые проверяют доступный контент, а также направляют действия, в которых участвуют пользователи. Помимо модераторов, приложение использует программное обеспечение для мониторинга и сотрудничает с несколькими организациями, которые способствуют безопасности детей в интернете, а также с правоохранительными органами.

Источники

1. Badillo-Urquiola, et al. «Stranger Danger! Social Media App Features Co-designed with Children to Keep them Safe Online». Association for Computing Machinery (2019)
2. Coughlan, Sean. «Safer Internet Day: Young ignore social age limit». BBC (2016), https://www.bbc.com/news/education-35524429
3. Kelly, Heather. «What parents need to know about social media for kids». The Washington Post (2021), https://www.washingtonpost.com/technology/2021/03/24/instagram-kids-faq/
4. Tartari, Elda. «Benefits and risks of children and adolescents using social media». European Scientific Journal vol. 11 No. 13 (2015)
5. «A parent’s guide to Internet Filtering and Monitoring». Axis (2018)
6. «A parents’ guide to filtering technologies. Get with it!» Brunswick Press Ltd. (2010)
7. «Children and parents: media use and attitudes report». Ofcom (2021)
8. «Children’s Online Privacy Protection Rule». Federal Trade Commission (2013), https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
9. «Social Media: help and advice». Childnet.com, https://www.childnet.com/help-and-advice/social-media/
10. «Social networks for kids and why they failed». Kaspersky (2016), https://kids.kaspersky.com/social-networks-for-kids/
11. «Teaching Kids to Be Smart About Social Media». KidsHealth.org (2020)
12. «The best social networks for younger children». Welivesecurity.com (2020), https://www.welivesecurity.com/2020/06/01/best-social-networks-younger-children/

3. Практики разработки

Пользовательский интерфейс должен предоставлять возможность блокировки некоторых функций во избежание запуска нежелательных действий и защиты детей от просмотра неприемлемой информации.

Зачастую существующие решения не блокируют, а ограничиваются лишь оповещением пользователей о возрастных ограничениях и содержании контента, в том числе о его потенциальной опасности. При этом ответственность за последующие действия на платформе, сайте или в приложении несет сам пользователь.

Наиболее распространенные механики, используемые для регулирования доступа к контенту:

- предоставление информации о контенте, например, возрастные рейтинги или дескрипторы контента;
- ограничение доступа несовершеннолетних по расписанию;
- ограничение доступа несовершеннолетних с помощью технических механизмов.

Информация о контенте используется для указания пригодности или вредоносности контента для детей. Система может состоять из возрастных рейтинговых меток, которые указывают на пригодность контента для различных возрастных категорий детей; может описываться характер контента и его характеристики — в форме надписей, текстовых указаний и предупреждений.

Ограничение доступа несовершеннолетних по расписанию используется для снижения вероятности того, что они будут подвержены воздействию потенциально опасного или неподходящего контента.

Технические меры включают механизмы, используемые для снижения вероятности того, что несовершеннолетние будут подвержены воздействию неподходящего контента путем создания технического барьера между пользователем и контентом. Наиболее распространенными примерами являются различные типы родительского контроля, PIN-коды или инструменты проверки возраста, например, проверки кредитных карт и проверки подтверждения возраста.

Технические меры защиты могут быть доступны пользователям для их добровольного использования, например, для родителей, которые хотят запретить своим детям просматривать неподходящий или опасный контент. А также могут быть обязательными для всех пользователей, например, обязательная форма подтверждения возраста.

Как правило, поставщики медиа-услуг могут включать информацию о контенте наряду с самим контентом в свои услуги, например, перед началом видео. Однако они часто полагаются на третьи стороны — стриминговые платформы, платформы для просмотра визуального, аудио- и видеоконтента, — чтобы обеспечить применение технических мер в своих сервисах. Поставщики контента аналогичным образом будут полагаться на авторов сервисов в отношении включения соответствующей информации о контенте, например, возрастных метках или текстовых указаниях.

Некоторые интернет-площадки проверяют сайты на наличие опасного программного обеспечения или исполняемых файлов и помогают предотвратить переходы по подозрительным ссылкам, которые могут нанести ущерб ее пользователям. Если площадка обнаружит угрозу для устройства при скачивании файла или переходе на подозрительный портал, то об этом появится предупреждение. Так, например, происходит на площадках Google и Mail.ru.

При этом существует несколько типов уведомлений о событиях, которые представляют опасность для пользователей:

1. предупреждение о вредоносном программном обеспечении, которое может автоматически установиться на компьютер;
2. предупреждение о том, что сайт может быть поддельным или подозревается в фишинге;
3. предупреждение о нежелательном программном обеспечении, которое может повлиять на работу браузера;
4. предупреждение о том, что посещение сайта небезопасно, т. к. страница сайта пытается загрузить скрипты[12] из непроверенных источников.

Согласно отчету Nielsen Norman Group, в рамках которого исследователи изучили вопрос о восприятии контента детьми в возрасте от 3 до 12 лет, были выделены следующие рекомендации по дизайну веб-сайтов и приложений:

1. Детям необходимо давать четкие и конкретные инструкции, обязательно указав цель и способ достижения онлайн-задач. Выяснилось, что дети в возрасте 5-6 лет легче адаптируются к онлайн-игре, если используются звуковые и визуальные инструкции. В противном случае при отсутствии связи между различными элементами ребенок может быть сбит с толку и не понять, какой результат ему необходимо достичь.

2. Все инструкции должны соответствовать уровню понимания детей. Предоставить инструкции недостаточно — дизайнеры также должны убедиться, что дети могут их понять.

3. Для помощи детям с выполнением заданий необходимо использовать существующие ментальные модели и знания о мире. Еще один способ воспользоваться существующими у детей ментальными моделями — это опираться на общие знания, которые у них уже есть из повседневной жизни.

4. Для снижения когнитивной нагрузки необходимо разрабатывать понятные интерфейсы, предотвращая возможные ошибки. У детей объем кратковременной памяти гораздо ниже, чем у взрослых, поэтому важно обращать внимание на то, чтобы интерфейс приложения был прозрачным и с понятной инструкцией. Дополнительно для снижения когнитивной нагрузки на детей используют предотвращение возможных ошибок. Так, компания Google при формировании поисковых запросов использует автокоррекцию, что помогает избежать неверных формулировок. В ходе тестирования выяснилось, что дети 5-11 лет сильно полагались на функцию автозамены поисковой системы, потому что они часто делали опечатки и испытывали трудности с правописанием.

5. Инструкции для детей должны быть четкими и конкретными, но не слишком предписывающими. Незрелость префронтальной доли коры головного мозга у детей означает, что они менее способны обрабатывать сложную и противоречивую информацию по сравнению с взрослыми. При разработке пользовательского интерфейса необходимо учитывать, что навыки рассуждения у детей все еще развиваются, поэтому они с большей вероятностью будут воспринимать конкретные инструкции буквально.

При разработке веб-сайтов, приложений и игр для детей важно помнить, что их когнитивные способности тоже находятся в процессе развития. Разница в возрасте также имеет большое

[12] Скрипт (англ. script «сценарий») — это небольшая программа, которая содержит последовательность действий, созданных для автоматического выполнения задачи.

значение при разработке пользовательского интерфейса, так как то, что работает для одной возрастной группы, не будет работать для другой.

Ограничения

Мошенничество

Несмотря на уведомления сайта об опасности действий, которые собирается совершить или совершил пользователь, дети все равно могут совершить переход по подозрительной ссылке, проигнорировать сообщение об угрозе или использовать инструменты для обхода ограничений и предупреждений.

В свою очередь, мошенники, преследуя цель обойти подобные механизмы, могут сделать это, например, с помощью редиректа[13] и короткого URL-адреса для перенаправления, которые являются эффективным способом распространения вредоносных файлов и программ.

Возрастная маркировка и деструктивный контент

Контроль доступа к взрослому контенту, не предназначенному для детей, может осуществляться несколькими способами, однако чаще всего это происходит с помощью возрастной маркировки и всплывающих уведомлений. При этом дети могут не обратить внимания на эти знаки или же осознанно проигнорировать их, например, указав неправильный возраст.

Технологий достоверной проверки возраста пользователя не существует. Всплывающее окно с запросом возраста необходимо администрации сайта — для них это способ переложить ответственность за просмотр и скачивание контента на пользователя.

Примеры

TikTok

Приложением TikTok могут пользоваться лица от 13 лет, поэтому при регистрации необходимо указать дату рождения. При этом минимальные возрастные ограничения не указываются, а также предотвращаются повторные попытки юных пользователей, не достигших 13 лет, пройти регистрацию.

У такого решения есть очевидный недостаток: ребенок может указать неверные данные и получить доступ к платформе. Однако средства модерации ресурса обучены выявлять нарушителей и блокировать их аккаунты.

Pikabu

Pikabu — популярный информативно-развлекательный ресурс, где любой желающий может опубликовать пост и обсудить его в комментариях. Ресурс обладает системой модерации, которая предупреждает пользователя, что он собирается опубликовать пост или отправить сообщение, которое нарушает политику платформы. Несмотря на то, что данная система не блокирует размещение контента, а лишь информирует о нарушении, такое решение может остановить взрослого или ребенка, от публикации недопустимого контента из-за угрозы

[13] Редирект — это перенаправление пользователя с одного URL на другой.

удаления и блокировке на платформе. Однако автоматическая система модерации может совершать ошибки и ограничивать доступ к контенту, который является безобидным.

Youtube Kids

В специальном приложении Youtube для детей, Youtube Kids, навигация упрощена благодаря большим кнопкам и меньшему количеству блоков контента на странице. Кроме того, настройки безопасности на платформе гарантируют, что пользователи младшего возраста имеют доступ только к предназначенному для них контенту.

Источники

1. Абдулаева Асият. «Ограничения права несовершеннолетних на получение и доступ информации». Проблемы совершенствования законодательства (2020)
2. Буети Кристина и др. «Руководящие указания для отрасли по защите ребенка в оналйновой среде». ITU
3. Официальный сайт YouTube Kids, https://www.youtube.com/kids/
4. Правила публикации контента Pikabu, https://pikabu.ru/information/rules
5. Справка Google о вредоносном и нежелательном ПО, https://developers.google.com/search/docs/advanced/security/malware?hl=ru
6. Справка о небезопасных сайтах Mail.ru, https://help.mail.ru/atom/safety/safe_browsing
7. «Как TikTok ограничивает доступ на платформу для пользователей младше 13 лет». TikTok, https://newsroom.tiktok.com/ru-ru/how-tiktok-prevents-using-the-platfrom-by-minor-users
8. Batt, Simon. «The Dangers of Shortened Links and How to Stay Safe». MakeTechEasier (2017), https://www.maketecheasier.com/dangers-of-shortened-links-and-stay-safe/
9. Nielsen, J. «UX Design for Children (Ages 3–12)». Nielsen Norman Group
10. Perez, Sarah. «YouTube to launch parental control features for families with tweens and teens». TechCrunch (2021), https://techcrunch.com/2021/02/24/youtube-to-launch-parental-control-features-for-families-with-tweens-and-teens/
11. «E-commerce: conversion thanks to real-time age verification». Deutsche Bank AG (2018), https://developer.db.com/products/dbAPI_CaseStudy_madco_EN.pdf
12. «Protection of Minors in the Audiovisual Media Services: Trends & Practices». ERGA, https://erga-online.eu/wp-content/uploads/2016/10/ERGA-PoM-Report-2017-wordpress.pdf

4. Инструменты родительского контроля и мониторинга

Инструменты родительского контроля предназначены для обеспечения безопасности детей в интернете. Они предоставляют родителям повышенную степень контроля над действиями детей в онлайн- и офлайн-среде благодаря установке специального программного обеспечения на смартфоны, компьютеры и другие устройства.

В базовый функционал инструментов родительского контроля входят:

- блокирование доступа к интернету, приложениям, играм;
- ограничение экранного времени;
- защита от ненадлежащего контента с помощью его фильтрации;
- отслеживание онлайн-активности, контактов и местоположения ребенка.

Эти функции обеспечивают проактивную регуляцию и мониторинг действий ребенка в интернете, поэтому такие программы позволяют минимизировать риски заблаговременно.

Родительский контроль может осуществляться непосредственно родителями или образовательным учреждением. Он может быть локальным или привязанным к устройствам, подключенным к мобильному интернету, а также объединять мобильные, локальные, стационарные устройства в единую систему контроля.

Приложения родительского контроля

Основным инструментом родительского контроля являются приложения, которые устанавливаются родителями на устройство ребенка. Функционал приложений родительского контроля может включать в себя доступ ко всем файлам на устройстве ребенка, контактам, переписка, звонкам, микрофону и видеокамере. Более того, современные версии таких инструментов способны определять смысл переписки и сообщать родителям о буллинге или домогательствах, блокировать съемку нецензурного контента, определять интересы ребенка и вычислять среди них опасные.

Встроенное программное обеспечение

Функции родительского контроля могут быть встроены по умолчанию в операционную систему устройств. Это делают производители телефонов, планшетов и игровых консолей, например: Apple, Amazon, PlayStation. Операционная система Android также обладает подобными функциями, несмотря на то, что она не эксклюзивна в плане производителя устройств.

Для активации данных инструментов требуется создать семейный аккаунт, где связываются несколько устройств и пользователей. Родительское устройство обладает административными правами, благодаря чему может регулировать доступ ребенка к приложениям, контенту и функциям.

Программное обеспечение для образовательных учреждений

Инструменты родительского контроля используются в образовательных учреждениях для фильтрации контента. При этом классный руководитель владеет доступом к информации об онлайн-активности ученика.

Когда в США участились случаи массовых расстрелов и суицидов среди несовершеннолетних, школы стали включать в свое программное обеспечение дополнительный функционал по

отслеживанию поисковых запросов и активности детей в социальных сетях. Мониторинг покрывает темы суицида, экстремизма, половых контактов и противозаконной деятельности. С помощью таких систем стало возможным предотвращение рисков на ранней стадии. Для выявления опасных слов и фраз используются лингвистический анализ, технологии машинного обучения и искусственного интеллекта.

У родителей также есть возможность подключиться к инструментам контроля от образовательных организаций. Так, в случае выявления риска или при обнаружении интереса ребенка к опасным темам, сигнал тревоги получают и родители, и администрация школы. При необходимости ребенку оказывает помощь психолог. При этом в особо опасных ситуациях администрация школы передает информацию в полицию.

Приоритеты для родителей

По результатам исследования, проведенного Роскачеством и компанией OMI, выяснилось, что 69 % родителей считают функции веб-фильтрации и защиты от сайтов с взрослым и опасным контентом наиболее востребованными. При этом возможность определения местоположения ребенка считают необходимым 67 % опрошенных. Эти две функции назвали основными как действующие пользователи приложений родительского контроля, так и те, кто только планирует начать ими пользоваться. При этом 60 % опрошенных отметили важность контроля за расходом средств и оплаты в приложениях, а 55 % считают необходимым мониторинг контактов, друзей и сообществ в соцсетях.

19 % родителей не используют инструменты родительского контроля, поскольку они слишком сильно ограничивают ребенка. 11 % признаются, что не устанавливают родительский контроль, так как это слишком сложно. 17 % родителей не видят в этом смысла, поскольку дети могут обойти ограничения. При этом 13 % утверждают, что это ограничивает их использование интернета.

По данным исследования компании «Лаборатория Касперского», 48 % из 11 000 опрошенных родителей в 19 странах используют приложения родительского контроля.

Вопросы кибербезопасности и конфиденциальности

Частные компании, предоставляющие сервис приложений родительского контроля, сталкиваются с проблемой безопасности персональных данных детей. По результатам исследования 14 наиболее популярных приложений родительского контроля, в 48 % случаях информация о пользователе передавалась без шифрования в процессе установки приложения, а в 28 % — происходила утечка информации о пользователе тогда, когда мониторинг уже был установлен.

По результатам другого исследования 46 приложений родительского контроля от 43 разработчиков, 11 % приложений передают личные данные в незашифрованном виде; 34 % собирают и отправляют личную информацию без соответствующего согласия; 72 % приложений передают данные третьим сторонам, включая службы онлайн-рекламы и аналитики, не упоминая их присутствие в своих политиках конфиденциальности.

Положительные эффекты

По данным компании Gaggle, которая осуществляет мониторинг более 5 млн учащихся в США, в 2019-2020 учебном году было обнаружено около 64 000 упоминаний о самоубийстве или членовредительстве, 5600 из которых были достаточно серьезными для немедленного

реагирования. При этом Gaggle помогла спасти жизни 927 учащихся, которые планировали или пытались совершить самоубийство.

По утверждению компании Bark, осуществляющей мониторинг 5,9 млн детей, за время своего существования с 2015 года система определила 490 000 серьезных ситуаций с самоповреждением и склонности к суициду у детей, а также 2,5 млн серьезных ситуаций буллинга.

Ограничения

Научные исследования показывают, что инструменты родительского контроля, которые позволяют осуществлять постоянное наблюдение за ребенком, разрушают доверие к родителям. Вторжение родителей в приватность социальной жизни детей влечет за собой также психологические травмы и депрессию. При этом систематический мониторинг онлайн-активности детей в учебных учреждениях негативно влияет на самовыражение, креативность и на ментальное здоровье ребенка в целом.

Введение контроля в подростковом возрасте без предыдущего опыта вызывает резкое неприятие и в целом негативное отношение детей старшего возраста к приложениям родительского контроля. Поэтому подростки находят способы обхода данных приложений.

Также ученые отмечают, что ребенок должен осознавать риски, с которыми он может столкнуться в интернете, и самостоятельно справляться с ними. При этом задача родителей — объяснить ребенку эти риски и научить пользоваться необходимыми инструментами. Пытаясь полностью оградить подростков от онлайн-рисков при помощи программ родительского контроля, некоторые родители не позволяют подросткам выработать необходимые механизмы выживания, которые понадобятся им на протяжении всей жизни.

Для настроек фильтрации в модемах, DNS, расширениях браузеров необходимы специальные навыки системного администрирования. Исследование выявило значительные трудности при настройке родительского контроля на большинстве устройств как со стороны родителей, так и со стороны детей.

Кроме того, наблюдаются несоответствия между ожиданием пользователей и реальной эффективностью. Основными проблемами являются слабая или чрезмерная работа алгоритмов и фильтрации. Стандартные фильтры блокируют порнографический и контент 18+ вполне корректно, однако исследование Оксфордского Университета указывает на то, что системы фильтров приложений родительского контроля при намеренном поиске такого контента подростками абсолютно неэффективны.

Примеры

Bark Technologies

Bark Technologies — сервис родительского контроля, предназначенный для родителей. Система позволяет отслеживать более 30 самых популярных приложений и платформ социальных сетей, включая обмен текстовыми сообщениями и электронную почту. Bark также анализирует поведение ребенка онлайн, составляя его расширенный психологический профиль, определяет интерес ребенка к противоправным действиям, склонность к ранним половым контактам, самоповреждению, суициду, пищевым отклонениям. Данные о рисках или отклонениях в

поведении передаются родителям в виде отчетов и сигналов тревоги для оказания своевременной помощи ребенку.

Kaspersky Safe Kids

Kaspersky Safe Kids — решение родительского контроля. Совместимо с операционными системами Windows, macOS, Android и iOS, работает на ПК, телефонах и планшетах. В функционал входит блокировка нежелательного контента, ограничение доступа к устройствам в соответствии с расписанием, ограничение доступа к приложениям, составление списка приложений, доступ к которым осуществляется с разрешения родителей, отслеживание местоположения ребенка по GPS, безопасный поиск и история активности на YouTube, контроль уровня заряда батареи.

Герда Бот

Герда Бот — российская система мониторинга активности детей в соцсети «ВКонтакте» с оповещением. Герда Бот формирует отчет о профиле в ВК со списком групп, списком ссылок, найденных опасных групп, в которых состоит ребенок, проверкой друзей ребенка на опасные группы, поиском скрытых аккаунтов ребенка. Есть версия для учебных заведений.

Источники

1. Официальный сайт проекта Герда Бот, https://gerdabot.ru
2. Официальный сайт сервиса Kaspersky Safe Kids, www.kaspersky.ru/safe-kids
3. Официальный сайт сервиса родительского контроля Bark Technologies, https://bark.us
4. Решетникова Мария. «Как настроить смартфон ребенка: родительский контроль и не только». РБК. Тренды (2022), https://trends.rbc.ru/trends/education/62036f839a7947d009ad568b
5. Справка Роскачества о родительском контроле (2020), https://rskrf.ru/ratings/tekhnologii/mobilnye-prilozheniya/roditelskiy-kontrol/
6. «Использование средств родительского контроля на iPhone, iPad и iPod touch ребенка». Служба поддержки Apple, https://support.apple.com/ru-ru/HT201304
7. «Исследование функциональности наиболее популярных мобильных приложений для родительского контроля для платформ iOS и Android». Центр цифровой экспертизы Роскачества
8. «Как настроить родительский контроль на консолях PS4». Служба поддержки PlayStation, www.playstation.com/ru-ru/support/account/ps4-parental-controls-and-spending-limits/
9. «Как управлять временем использования устройств и приложений». Служба поддержки Google, https://support.google.com/families/answer/7103340?hl=ru
10. Bell, Terena. «How Software is taking on school shootings». FastCompany (2017), www.fastcompany.com/40477172/could-software-stop-school-shootings
11. Brown, Marquita. «K-12 leaders weigh threats and benefits of increased web monitoring». EdTech Magazine (2019)
12. Coxner, M. and Narva Jacobsson, S. «Parental privacy invasions and adolescent depressive symptoms». Orebro University (2018)
13. D'Haenens, Leen, et al. «How to cope and build online resilience?» (2013)
14. Feal Fajardo, Alvaro. «Study on privacy of parental control mobile applications». IMDEA Software Institute (2017)
15. Feal, Alvaro. «Angel or devil? A privacy study of mobile parental control apps». Proceedings on privacy enhancing technologies (2020)

16. Ghosh, Arup Kumar. et al. «Safety vs. surveillance: what children have to say about mobile apps for parental control». Univercity of Central Florida, www.eecs.ucf.edu/~jjl/pubs/pn1838-ghoshA.pdf
17. Hawk, Skyler, et al. «Adolescents' perceptions of privacy invasion in reaction to parental solicitation and control». The Journal of Early Adolescence 28 (4) (2008)
18. Kamenetz, Anya. «To prevent school shootings, districts are surveilling students' Online Lives». NPR (2019), www.npr.org/2019/09/12/752341188/when-school-safety-becomes-school-surveillance
19. Knorr, Caroline. «Parents' Ultimate Guide to Parental Controls». Common Sense Media (2021), www.commonsensemedia.org/articles/parents-ultimate-guide-to-parental-controls
20. Kolodny, Lora. «Securly raises $4 million to put guard rails on the internet for K-12 students». TechCrunch (2016), https://techcrunch.com/2016/10/20/securly-raises-4-million-to-put-guard-rails-on-the-internet-for-k-12-students/
21. Komar, Olha A., et al. «Implementation of a Monitoring System in the Educational Process in Primary School». International Journal of Learning, Teaching and Educational Research Vol. 18 No. 11 (2019)
22. Leibowitz, Aaron. «Could monitoring students on social media stop the next schhol Shooting?» The New York Times (2018), www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html
23. Livingstone, Sonia and Ellen Helsper. «Parental mediation and children's Internet use». Journal of broadcasting and electronic media 52 (4) (2008)
24. McFarlin, L.A., et al. «Usability Impact on Effectiveness of Parental Controls». Proceedings of the Human Factors and Ergonomics Society Annual Meeting (2007)
25. Przybylski, A. K. et Victoria Nash. «Internet filtering and adolescent exposure to online sexual material». Cyberpsychology, behavior and social networking Vol. 21 No. 7 (2018)
26. Shek, Daniel T. L., et al. «The influence of parental control and parent-child relational qualities on adolescent internet addiction: a 3-year longitudinal study in Hong Kong». Frontiers in psychology (2018)
27. Stark, Phillip B. «The effectiveness of internet content filters». University of California (2007)
28. Wisniewski, Pamela, et al. «Parental control vs. teen self-regulation: is there a middle ground for mobile online safety?» ACM Conference on computer supported cooperative work and social computing (2017)
29. «How to prevent your kids from bypass parental controls». TechTricksZone (2021), https://techtrickszone.com/prevent-your-kids-from-bypass-parental-controls/
30. «Internet monitoring software to control cyber-bulling In schools». PearlSoftware, www.pearlsoftware.com/solutions/cyberbullying-in-schools.html
31. «Online security apps focus on parental control, not teen self-regulation». Science Daily (2017)
32. «Overblocking and underblocking in network level filters». Parliament UK, https://publications.parliament.uk/pa/cm201617/cmpublic/digitaleconomy/memo/DEB63.pdf
33. «Parental Controls», Childnet, www.childnet.com/help-and-advice/parental-controls/
34. «Perfomance report». AEPD (2021), www.aepd.es/sites/default/files/2020-04/nota-tecnica-protection-of-minors-on-the-internet-en.pdf
35. «Raising the smartphone generation. New research into how parents and children manage their digital habits». Kaspersky (2021), www.kaspersky.com/blog/digital-habits-report-2021/
36. «Set Up Parental Controls on Your Fire Tablet». Amazon, www.amazon.com/gp/help/customer/display.html?nodeId=GG2LBLF5V2T8XUX8
37. «Views on student activity monitoring software». Center for democracy and technology (2021), https://cdt.org/wp-content/uploads/2021/09/Student-Activity-Monitoring-Software-Polling-Research-Slides.pdf

38. «What Bark monitors». Официальный сайт сервиса родительского контроля Bark Technologies, https://bark.us/what-bark-monitors

5. Интернет-фильтры

Интернет-фильтры — это инструменты, которые позволяют предотвратить либо загрузку опасного контента на серверы, либо попадание такого контента в поле зрения ребенка. В отличие от автоматизированной модерации, такие фильтры не привязаны ко времени реагирования команды модераторов — они либо защищают ребенка постоянно, либо изначально не позволяют загружать некоторые виды контента на серверы.

Средства фильтрации могу представлять собой аппаратно-программные комплексы, которые ограничивают доступ к сайтам и контенту, если они представляют угрозу здоровому развитию детей или нарушают законы, установленные в государстве.

Интернет-фильтры позволяют ограничивать доступ к нежелательным для ребенка ресурсам и блокировать скачивание вредоносных файлов. Также существуют программы, определяющие опасный для детей контент по ключевым словам, что позволяет обеспечить защиту ребенка от наиболее опасных элементов интернета.

Фильтрация контента может осуществляться как на уровне отдельных пользователей, когда на устройства устанавливается специальная программа, так и на глобальном уровне, где сетевой трафик от всех пользователей собирается различными методами и фильтруется.

Более 78 % опрошенных в 2016 году родителей уверены в том, что их дети не могут обойти установленную для них фильтрацию контента. Для сравнения в 2015 году этот показатель был равен 67 %. Что интересно, 8 % из опрошенных родителей не имеют представления, способны их дети обойти фильтры или нет.

Опрос родителей с детьми в возрасте от 4 до 16 лет показал, что только 39 % родителей настраивают фильтры для роутеров и Wi-Fi в домашней сети, 35 % устанавливают родительский контроль на домашних устройствах.

Ограничения

Интернет-фильтры также имеют свои недостатки: например, некорректное распознавание определенных слов или фраз, которые ошибочно воспринимаются системой как непристойные — это явление называется «проблемой Скантorп» (от англ. scunthorpe problem). Эта проблема возникает из-за особенностей интерпретации контекста компьютером, что приводит к ложным срабатываниям и блокировке. Например, сервис для сравнения цен на товары на онлайн-площадках Google Shopping ошибочно исключил из своей выдачи всю продукцию, которая включала в себя слово gun (англ. оружие) в названии. Среди таких товаров оказались водяные пистолеты (англ. water gun), бургундское вино (англ. burgundy wine) и даже диски рок-группы Guns N’ Roses.

Исследования подтверждают, что фильтры не влияют на вероятность столкновения ребенка с худшими сторонами интернета. Более того, у детей, которые пользуются устройствами с фильтрацией интернета, менее развиты технические знания, и они незначительно чаще становятся жертвами злоумышленников онлайн. В целом дети из семей, пользующихся интернет-фильтрами, сообщали о том, что они стали жертвой злоумышленников на 10 % чаще. Скорее всего, это связано с тем, что ребенок, чей интернет полностью фильтруется, растет в «тепличной» среде и не может видеть, как другие люди становятся жертвами мошенников, не узнает о методах злоумышленников, и, следовательно, не может их распознать. Ученые также

отметили, что излишняя фильтрация может помешать ребенку найти полезную и релевантную информацию о своих проблемах.

Примеры

Яндекс.DNS

Яндекс.DNS — это бесплатный сервис фильтрации контента, основанный на настройках DNS и модема. Он блокирует вредоносные сайты, контент, нежелательный для просмотра детьми, а также сайты мошенников, содержащие фишинг. Сервис защищает все устройства домашней сети.

NetPolice Pro

NetPolice Pro — это интернет-фильтр, обладающий гибкими настройками, которые можно легко менять вручную. Фильтрация отталкивается от рекомендаций Минобрнауки РФ. Программа способна самостоятельно проверять контент сайтов и блокировать их, исходя из составленных самим пользователем белого и черного списков.

Traffic Inspector

Traffic Inspector — это система безопасности, обеспечивающая контроль и защиту доступа к интернету в корпоративной сети. Программа поддерживает фильтрацию «черных» и «белых» списков. Ведется статистика посещений пользователей различных сайтов. В дополнение к основному продукту имеются модули расширения для фильтрации рекламы, фишинга, проверка трафика через антивирус, контентная фильтрация.

SkyDNS

В программе SkyDNS есть возможность распределить сайты по категориям, ограничив доступ ребенка к тем из них, которые не подходят ему по возрасту или по другим причинам. В распоряжении родителей есть статистика посещенных сайтов, очистка рекламы от порнографии и другого шокирующего контента. Программа также позволяет блокировать ресурсы, нацеленные на взлом посетителей, мошенничество, кражу денег и персональных данных. Ребенок, перейдя на подобный сайт, увидит предостерегающую надпись, а доступ к сайту будет заблокирован.

Cyacomb Safety

Cyacomb Safety — это технология, позволяющая пропускать через фильтр, базирующийся на базе данных вредоносного контента, весь загружаемый пользователями контент на любой площадке. Процесс фильтрации происходит в режиме реального времени. У пользователей есть возможность самостоятельно добавлять в эту базу новые фильтры и сообщать правоохранительным органам о происшествии. Весь процесс модерации происходит без ущерба для конфиденциальности пользователей.

Lidrekon

Lidrekon — это расширение для браузеров, позволяющее фильтровать контент. Проверка контента происходит на основе российской библиотеки фильтров, которая постоянно обновляется. Расширение фильтрует контент по темам: членовредительство, суицид, ПАВ,

наркотики, табак, алкоголь, азартные игры, проституция, бродяжничество, оправдание насилия к людям и животным, отрицание семейных ценностей, нетрадиционные ориентации, неуважение к детям и родителям, криминал, оружие, нецензурная брань, порнография, экстремизм. Может быть установлено как на домашних устройствах, так и в учебных заведениях, библиотеках.

Источники

1. Емельянов Дмитрий Александрович. «Фильтрация сетевого контента в образовательных учреждениях». Педагогическое образование в России 8 (2018).
2. Официальный сайт интернет-магазина Netpolice, https://www.netpolice.ru/
3. Официальный сайт компании Cyacomb, https://cyacomb.com/cyacomb-safety/
4. Официальный сайт компании Smart-soft, https://ti.smart-soft.ru/solutions/firewall-ngfw/
5. Официальный сайт сервиса Lidrekon, https://lidrekon.ru/block/
6. Официальный сайт сервиса SkyDNS, https://www.skydns.ru/
7. Официальный сайт сервиса Яндекс.DNS https://dns.yandex.ru
8. Перевозчикова Марина и Антон Сапегин. «Способы контроля доступа школьников к компьютерным ресурсам». Концепт 10 (2014)
9. «Обзор перспектив блокировки интернет-контента». ISOS, Internet Society (2017)
10. Keller, Daphne. «Facebook Filters, Fundamental Rights, and the CJEU’s Glawischnig-Piesczek Ruling». GRUR International 69.6 (2020)
11. Livingstone, S., et al. «Children’s online activities, risks and safety». UKCCIS (2017)
12. Molloy, Mark. «Wine lovers cannot buy Burgundy tipple on Google as internet giant cracks down on 'gun' searches». The Telegraph, (2018)
13. Przybylski, A. K. and V. Nash. «Internet Filtering Technology and Aversive Online Experiences in Adolescents» (2017)

6. Автоматизированная модерация

Модерация — комплекс мероприятий, направленных на выявление нарушения пользователем общепринятых правил. Также под модерацией контента понимают применение набора правил или стандартов для публикуемого контента, который может проявляться во многих форматах (таких как текст, изображения, видео или аудио), на любую тему, потенциально на любом языке или диалекте, из тысяч или миллионов культурных контекстов.

Модерация контента включает в себя удаление информации, ее фильтрацию или блокировку, рекомендацию контента через новостные ленты, тематические списки и персонализированные предложения, а также мониторинг контента.

У ручной модерации есть несколько серьезных ограничений. Во-первых, штат модераторов ограничен, во-вторых, каждый модератор подвержен фактору человеческой ошибки, в-третьих, объем контента, который модератор может проверить, серьезно ограничен. В зависимости от особенностей платформы могут появляться и другие проблемы. Например, закрытые микросообщества, которые распространяют нелегальные материалы и существуют продолжительное время, потому что никто не отправляет жалобу.

Автоматизация модерации решает многие из этих проблем, так как программа может сканировать все происходящее на платформе, в отличие от обычных модераторов, которым приходится полагаться на жалобы и патрулирование разделов платформы. Автоматизация в модерации контента может использоваться на соответствующих этапах превентивного обнаружения потенциально проблемного контента, а также для автоматизированной оценки и исполнения решения об удалении, маркировке или демаркировке, демонетизации или приоритизации контента.

Предварительная модерация помогает производить проверку материала перед публикацией, контролировать качество контента и применять в отношении нарушителей правил портала ограничительные меры. При постмодерации происходит проверка контента уже после его публикации на платформе.

С помощью специальных программ и методов фильтрации при автоматической модерации происходит проверка контента по соответствующим критериям. Также функции автомодерации частично могут взять на себя сами пользователи, помогая оценить практическую пользу и качество предлагаемого контента. В случае жалоб пользователей может производиться модерация конфликтов.

Важным вопросом модерации контента на любом уровне является определение вредоносного контента:

- контент, который считается неприемлемым и/или опасным для определенного интернет-ресурса;
- контент, который явно запрещен законом, и его распространение для всех групп лиц;
- запрещенный контент и тот, который может быть формально законным, но распространение которого представляет опасность для отдельных категорий лиц, например, неприемлемый для несовершеннолетних контент.

Опыт Meta (ex. Facebook)*

По утверждениям компании Meta*, искусственный интеллект способен распознать около 100 % спама, а также более 95 % контента, связанного с терроризмом, фейковыми аккаунтами и материалов сексуального характера. При этом искусственный интеллект может выявлять без помощи модераторов более 85 % графических изображений, на которых присутствуют сцены насилия.

Согласно внутренней статистике, на одну ошибку модерации приходится более 100 постов с запрещенным контентом, удаленных еще до того, как их кто-нибудь увидел. Но если порнографические материалы и спам искусственный интеллект почти искоренил, то с обработкой человеческой лексики возникают трудности. К тому же до сих пор нет общепринятых стандартов: что считать проявлением ненависти, а что нет. Поэтому сейчас искусственный интеллект распознает лишь 38 % оскорбительных постов (чаще всего на английском или португальском языке).

Опыт Google

Безопасный поиск в Google взаимосвязан с безопасным режимом в YouTube: при включении первой функции автоматически активируется вторая и наоборот. Вместе с тем в YouTube действует ряд правил, призванных обеспечить безопасность детей, использующих сервис.

Принципы сообщества YouTube запрещают размещение видеороликов следующего характера:

- Порнография и сцены откровенного сексуального содержания (даже если на видео сам автор ролика).
- Сцены употребления наркотиков и изготовления бомб.
- Сцены беспричинного насилия, в том числе его провоцирующие, причинения боли, нападений, оскорблений, грубого обращения с животными.
- Жестокие видео несчастных случаев, смерть и т. д.
- Материалы, нарушающие авторские права, в том числе музыкальные дорожки и фрагменты программ, защищенные авторским правом.
- Материалы, разжигающие нетерпимость: «высказывания, направленные на группу, с апелляцией к таким понятиям, как расовое или этническое происхождение, религия, ограниченная дееспособность, пол, возраст, статус ветерана, сексуальная ориентация или половая самоидентификация».

Все материалы, нарушающие перечисленные выше правила, удаляются, а аккаунты, размещающих их пользователей, блокируются. В случаях, когда контент противоречит законам, информацию передают в правоохранительные органы (в первую очередь речь идет о материалах, связанных с похищением и сексуальной эксплуатацией детей).

Эффективность использования

Некоторые крупные интернет-сообщества разрабатывают собственную информационную политику, определяют виды контента и основные требования к размещаемой информации, нарушение которых может послужить основанием для блокировки сайта или канала. На сегодняшний день существует ряд решений для борьбы с распространением опасного контента, но они работают только с определенной частью проблемы, не охватывая ее полностью.

Ограничения

Преимущество ручной фильтрации заключается в относительной точности, верифицируемости результатов удаления материалов, а также возможности улучшения критериев для блокировки. Механизмы автоматической фильтрации более действенны, однако они с большей вероятностью могут посягнуть на свободу выражения и поиска информации.

Что касается существующих средств автоматической модерации текстового контента, то такие, обычно платные средства, либо имеют ограничения по количеству транзакций, обрабатываемых в единицу времени, либо не способны поддерживать обработку русского языка.

Для обхода систем автомодерации содержимого широко используются варианты изменения данных, включающие в себя, например, введение дополнительных пробелов, отсутствие пробелов, использование транслитерации. При этом система будет устойчива к такому набору входных данных, если к автоматической фильтрации добавить возможность вручную генерировать изменения и дополнять ими обучающую выборку. Чтобы обойти автоматическую модерацию на предмет использования нецензурной лексики, авторы текстов модифицируют ее, удаляя, заменяя или добавляя те или иные графемы, используя знаки препинания или латиницу вместо кириллицы.

Примеры

Meta (ex. Facebook)*

Meta* использует автомодерацию, чтобы выявлять спам, фейковые страницы, порнографию, экстремистские материалы, ролики со сценами жестокости. Однако на сегодняшний день алгоритмы не способны точно распознавать призывы к осуществлению экстремистской деятельности — этим занимаются модераторы. В Instagram* внедрена программа DeepText на базе ИИ для фильтрации травли и издевательств. Изначально она искала только спам, потом научилась обнаруживать оскорбительные комментарии, а затем инструмент начали обучать анализу не только комментариев, но и постов.

Microsoft

Azure Content Moderator — это сервис на базе ИИ, позволяющий управлять контентом, который может быть оскорбительным, представлять опасность или быть нежелательным по какой-либо другой причине. Он включает службу контроля содержимого на основе искусственного интеллекта, которая сканирует текст, изображение и видео и автоматически применяет флаги содержимого.

PhotoDNA — это технология, разработанная и принадлежащая компании Microsoft, которая используется для борьбы с распространением незаконных изображений, видео и аудиофайлов. Программа автоматически сканирует загружаемые фотографии, чтобы распознать и уведомить о присутствии на снимках порнографического содержания с участием несовершеннолетних. Система не удаляет, а помечает изображения, таким образом, последующей проверкой и блокировкой занимается человек, что не только замедляет процесс, но и дает возможность злоумышленнику получить фото и распространить его на другие ресурсы.

Источники

1. Бутаев Михаил Матвеевич, Алексей Иванович Мартышкин. «Основные методы автоматической обработки и модерации текстовых данных в социальных сетях». XXI век: итоги прошлого и проблемы настоящего плюс 10.2 (2021): 30-34.
2. Добринская Дарья Егоровна. «Что такое цифровое общество?». Социология науки и технологий 12.2 (2021): 112-129.
3. Комалова Л. Р. «2015. 01. 013-015. Интернет-коммуникация с элементами речевой агрессии. (Сводный реферат)». Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 6, Языкознание: Реферативный журнал 1 (2015).
4. Миюзов Роман Евгеньевич. «Применение технологии искусственного интеллекта при модерации контента в сети интернет». Студенческая наука: актуальные вопросы, достижения и инновации (2021).
5. Научно-технический центр ФГУП «ГРЧЦ», Правовое регулирование защиты несовершеннолетних пользователей сети «Интернет» от вредоносного контента (2021), https://rdc.grfc.ru/2021/08/minors_law_protection/
6. Официальный сайт «Microsoft», https://www.microsoft.com/en-us/photodna
7. Плотников Г. И. «Система автоматической модерации текста на основе искусственных нейронных сетей». Вестник современных исследований 12.1 (2018): 641-645.
8. Понарина М. С. и М. В. Янаева. «Основные направления поиска потенциально опасного контента в социальных сетях». Технологические инновации и научные открытия (2021)
9. Тарасова Н. В., И. П. Пастухова и С. Г. Чигрина. «Индивидуальная программа развития и система наставничества как инструменты наращивания профессиональных компетенций педагогов. Рекомендации для руководящих и педагогических работников общеобразовательных организаций» (2020)
10. Толоконникова А. В. «Безопасность детей в интернете: основные сферы сетевого регулирования и саморегулирования». И безопасность детей (2018): 70.
11. Kertysova, Katarina. «Artificial intelligence and disinformation: How AI changes the way disinformation is produced, disseminated, and can be countered». Security and Human Rights 29.1-4 (2018): 55-81
12. Meta (ex. Facebook), «Introducing DeepText: Facebook’s text understanding engine» (2016), https://engineering.fb.com/2016/06/01/core-data/introducing-deeptext-facebook-s-text-understanding-engine/

7. Сервисы оказания помощи

Сервисы оказания помощи включают в себя спектр организаций и сервисов, которые позволяют ребенку, родителю или иным заинтересованным лицам запросить помощь психологов, волонтеров, правозащитников и других специалистов.

Сервис оказания помощи (платформа реагирования) — организация или сервис, целью которой является оказание поддержки уязвимым и пострадавшим детям. Они могут служить для оказания психологической помощи, коммуникаций между детьми и государством, НКО, волонтерами. Такие организации активно используют технологии и внедряются в инфраструктуру, которая касается поддержки детей. Одной из задач платформ реагирования также является просвещение общественности по вопросам помощи детям.

Многие платформы реагирования подразумевают несколько каналов для коммуникации с детьми: телефон доверия, сайты, мессенджеры, чат-боты. В зависимости от размеров и технических возможностей организации, количество и пропускная способность таких каналов варьируются. Чаще всего встречаются следующие виды технологических решений.

Телефон доверия — дистанционная служба экстренной психологической помощи, предназначенная для оказания моральной, эмоциональной или духовной поддержки широким слоям населения. На территории России этот термин применяется как к службе экстренной психологической помощи, так и к телефонным службам государственных организаций, которые собирают и предоставляют населению различную информацию.

Сайты — используются как способ предоставления контактов и информации о своей деятельности, распространения информационных материалов на тему поддержки детей в трудных ситуациях.

Мессенджеры — в популярных мессенджерах подобные организации создают группы, в которых размещают релевантную информацию, а также напрямую общаются с детьми, которые нуждаются в помощи.

Чат-боты — позволяют автоматизировать работу с запросами и избежать перегрузки специалистов. Использование таких программ оптимизирует рабочие процессы организации, а главное — позволяет оказать помощь своевременно и точно. Иногда они служат дополнительным способом донесения полезной информации с целью предотвращения потенциальных проблем, а также для просвещения детей и взрослых.

Организации, оказывающие подобные услуги, могут работать как с квалифицированными специалистами, так и с волонтерами. Обеспечение связи с детьми — одно из главных направлений деятельности и развития таких организаций. Существуют исследования, которые доказывают, что данные организации являются критически важным органом по защите детей.

Подобные организации обладают рядом преимуществ:

1. анонимность — телефоны доверия предоставляют полную анонимность людям, обратившимся за помощью;
2. доступность — звонок в подобные службы абсолютно бесплатен с любого устройства и из любого региона страны, при этом часть организаций работает круглосуточно;
3. открытость — платформы реагирования оказывают помощь всем обратившимся людям, вне зависимости от их пола, возраста, статуса и жизненных обстоятельств;

4. комплексность — в случае, если человеку необходима дополнительная или комплексная помощь, консультанты подключат необходимых специалистов для помощи пострадавшему;
5. оперативность — формат онлайн-взаимодействия со службами помощи подразумевает оперативность реагирования на инциденты, дети и подростки могут обратиться за помощью в тот же момент, как она им понадобилась.

По данным Федеральной службы государственной статистики Российской Федерации в 2021 году на территории страны проживает 33 млн детей, на которых приходится 220 служб телефона доверия.

Австралийская компания Kids Helpline ведет статистику по передаче заявок полиции и скорой помощи от горячих линий для детей. С декабря 2020 года до мая 2021 года телефонные службы помощи обращались в полицию или скорую помощь на 99 % чаще, чем в тот же период прошлого года.

Австралийская компания eSafety Commissioner выявила, что дети зачастую пытаются справиться со своими проблемами самостоятельно из-за того, что не знают, к кому обратиться, или ищут информацию в недостоверных, но комфортных для них источниках. Только 24 % из опрошенных детей в возрасте от 8 до 17 лет обратились бы в специализированную организацию, 51 % занимались бы решением проблемы сами, а 71 % выбрали бы наиболее комфортный путь поиска решений в знакомых для них источниках. Что примечательно, 50 % детей сами бы давали советы пострадавшему, и только 16 % предложили бы обратиться в специализированные организации.

Дети подвергаются трудностям не меньше взрослых и нуждаются в помощи — это подтверждает отчет общероссийского детского телефона доверия. В 2019 году было совершено около 900 тысяч звонков от детей, попавших в трудную жизненную ситуацию. Проблемы могли нести различный характер, от незначительного до критичного — более 8,5 тысяч раз дети звонили с намерением покончить жизнь самоубийством.

В США в 2020 году благодаря специальной горячей линии было зарегистрировано 10 583 случаев торговли людьми, из которых 2488 связаны с несовершеннолетними.

По данным российской линии помощи «Дети Онлайн», в период с 2010 года по 2014 год самыми распространенными обращениями детей были проблемы, связанные с коммуникаций и общением. Чуть менее распространены риски, вызванные различными техническими проблемами, в том числе связанные с мошенничеством или другими негативным воздействиям.

Ограничения

Несмотря на все преимущества, у традиционных платформ реагирования есть ряд ограничений.

Компетентность специалистов — сотрудники подобных организаций должны оказывать помощь людям, попавшим в самые сложные жизненные ситуации. Поэтому для корректной работы платформ реагирования требования к профессионализму операторов должны быть достаточно высокие.

Риск взлома или утечки — хранящиеся у горячих линий и НКО данные могут быть украдены. Чат-боты, телефоны и даже базы данных экстренных служб могут иметь уязвимости. Учитывая

то, что им нередко передается конфиденциальная информация, при успешном взломе злоумышленник может нанести ущерб пострадавшим и организации.

Проблемы в коммуникации — дети не всегда способны конкретно и четко описать проблему. Кроме того, анонимность контакта является палкой о двух концах: в экстренном случае может быть сложнее выслать помощь оперативно, если ребенок, обратившийся за помощью, совершил анонимный звонок.

Примеры

Child Helpline International

Child Helpline International — это международный ресурс, на котором опубликованы номера телефонов служб поддержки для детей. Имеет большое количество справочных материалов для детей и родителей.

Телефон доверия

Всероссийская телефонная линия помощи детям, оказавшимся в различных трудных жизненных обстоятельствах. Также на сайте организации ребенок может найти релевантные справочные материалы.

Чат-бот «Трудно подросткам»

«Трудно подросткам» — это чат-бот, позволяющий детям, пострадавшим от травли, обратиться за помощью. Бот способен перенаправлять запросы о помощи к организациям и индивидуальным специалистам. Он определяет проблему ребенка и потом направляет справочные материалы, контакты специалистов и профильных служб.

CyberTipline

CyberTipline — это система для государственных учреждений и поставщиков ИТ-сервисов. Предназначена для подачи жалоб и информации о насилии над детьми. Работает с составлением базы данных для анализа, поиска пострадавших, обучения нейросетей.

В 2020 году CyberTipline получила более 21,7 млн отчетов. Большая их часть касалась сексуального насилия и эксплуатации. Через CyberTipline поступило 65,4 млн файлов к рассмотрению, из них 31,7 млн видео и 33,7 млн изображений.

Источники

1. Михайлова Е.А. «Телефоны доверия как инструмент профилактики социального неблагополучия» Мониторинг общественного мнения: экономические и социальные перемены (2013): 109-113.
2. РОССТАТ «Численность населения Российской Федерации по полу и возрасту» (2021)
3. «За 2019 год на детский телефон доверия позвонили почти 900 тыс. раз». Агентство социальной информации, (2020), www.asi.org.ru/news/2020/02/05/za-2019-god-na-detskij-telefon-doveriya-pozvonili-pochti-900-tys-raz.
4. Child Helpline International, https://www.childhelplineinternational.org
5. EAB «Pros and cons of virtual mental health services according to experts»
6. eSafety Commissioner. «State of Play – youth, kids and digital dangers» (2018)

7. M. Emmison, S. Danby. «Troubles Announcements and Reasons for Calling: Initial Actions in Opening Sequences in Calls to a National Children's Helpline» (2007)
8. M. Hasal, J. Nowaková et al. «Chatbots: Security, privacy, data protection, and social aspects» (2021)
9. N. Petrowski, C. Cappa, A. Pereira, H. Mason, R. A. Daban; (2021)
10. National center for Missing & Exploited children «CyberTripline», https://www.missingkids.org/gethelpnow/cybertipline
11. National Human Trafficking Hotline. «Hotline Statistics» (2020)
12. NBC News «Hackers have taken down dozens of 911 centers. Why is it so hard to stop them?» (2018)
13. «New Kids Helpline Data Reveals Spike in Duty of Care Interventions», Yourtown (2021), www.yourtown.com.au/media-centre/new-kids-helpline-data-reveals-spike-duty-care-interventions.
14. «Violence against children during COVID-19: Assessing and understanding change in use of helplines, Child Abuse & Neglect»

8. Инфраструктура

Инфраструктура — это совокупность взаимосвязанных объектов, структур, решений безопасности, интегрированных в единую систему. Основной принцип обеспечения безопасности заключается в непрерывности защиты в пространстве и времени.

Инфраструктура объединяет ресурсы и пространства через интеграцию систем друг с другом. Под ресурсами понимаются различные технические и аппаратные средства, программное обеспечение и базы данных, каналы и средства связи и т.д. Пространства в свою очередь включают в себя различные физические объекты, начиная от места проживания ребенка, заканчивая общественными местами, транспортом, учебными заведениями и городом в целом.

Риски, с которыми дети сталкиваются в интернете, могут перетекать в офлайн и напрямую угрожать безопасности ребенка, в том числе в учебных заведениях. Локально на каждом объекте, в зависимости от принятых стандартов и индивидуальных инициатив образовательных организаций, могут устанавливаться различные решения, позволяющие обеспечить безопасность ребенка. Инфраструктура, адаптированная для детской безопасности и интегрированная с другими технологическими средствами, является залогом успешной борьбы с интернет-рисками для детей.

Видеонаблюдение и видеоаналитика

Видеонаблюдение может помогать контролировать безопасность детей. Для таких систем существует специальное программное обеспечение, которое сигнализирует о движениях или предупреждает о появлении в заданном периметре посторонних людей. Особенно часто подобные системы используются в случаях, когда ребенок на долгое время остается дома без родителей. Помимо этого, данные с наружных камер наблюдения и видеодомофонов могут использоваться в качестве доказательной и аналитической базы для правоохранительных органов при необходимости.

Помимо дома системы видеонаблюдения также используют в детских образовательных учреждениях. Для защиты детей в школах и детских садах создаются системы безопасности, оперирующие в едином стандарте, обозначенном региональными властями или государством. Такой стандарт позволяет объединять школы в единую систему наблюдения и синхронизировать их с городскими экстренными службами, полицией, МЧС, а также с инфраструктурой безопасности города: городское видеонаблюдение, каналы связи и т. д. В настоящее время в РФ существуют строгие требования по антитеррористической безопасности для учебных заведений.

Системы видеонаблюдения могут устанавливаться как внутри помещений, так и снаружи. Контроль прилегающей территории позволяет обеспечить видеонаблюдение по всему периметру, фиксировать все действия посетителей и прохожих.

Следуя концепции непрерывности в пространстве, камеры видеонаблюдения должны обеспечивать максимальное покрытие и устанавливаться таким образом, чтобы можно было проследить перемещения человека, последовательность действий и восстановить события. По сохраненным записям можно восстанавливать ход событий, проводить расследования для наказания виновных. Но безопасность детей в школах и детских садах должна быть проактивной и работать на предупреждение. Видеонаблюдение и в целом все системы должны предотвращать опасные ситуации и обеспечивать максимально быстрое реагирование.

Системы видеонаблюдения, установленные в образовательных учреждениях, позволяют:

- обнаружить попытки проникновения неизвестных подозрительных лиц;
- предотвращать террористические акты;
- выяснять причины травмы ребенка;
- выяснять обстоятельства кражи или порчи имущества и других противоправных действий;
- выявлять превышения полномочий персонала, преподавателей;
- выявлять и пресекать конфликтные ситуации между детьми;
- предотвращать случаи буллинга и насилия над детьми;
- предотвращать и выявлять случаи обращения наркотических средств, вовлечения учеников в употребление и распространение, а также обнаруживать факты курения и употребления алкоголя.

Обнаружение и предотвращение при этом полностью зависит от действий сотрудников охраны, работающих в учебном заведении. Человеческий фактор в такой системе — это ее частичная уязвимость. Обнаружение полностью зависит от наблюдательности сотрудников, смотрящих в мониторы, по большей части в течение 8-часового рабочего дня. Поэтому видеонаблюдение является пассивным средством предотвращения инцидентов, а охрана объекта — активным, но полностью находящимся в зависимости от человеческого фактора. Решить эту проблему помогают современные передовые технологии.

Технологии искусственного интеллекта, глубокого обучения и компьютерного зрения, встраиваемые в системы видеонаблюдения, должны решить вопрос частичной автоматизации для выявлении подозрительных ситуаций при считывании данных с множества видеокамер. Искусственный интеллект и алгоритмы видеоанализа способны даже выявлять конфликтные ситуации между школьниками.

Биометрия

В систему видеонаблюдения может быть интегрирована система распознавания лиц. Это один из функционалов видеоаналитики, позволяющий идентифицировать личность человека, вести подсчет людей в помещении. Идентификация проходит через сверку с данными из базы биометрии.

Система биометрической аутентификации используется для распознавания личности человека по характерным только для него признакам. В биометрию входят трехмерное сканирование лица, сетчатки глаза, дактилоскопия, снимок рисунка вен ладони, запись голоса, характеристики движения тела и походки, генетический тест. Биометрические данные используются для системы распознавания лиц и пропускных систем.

Базы данных и ЦОД

В Российской Федерации все биометрические данные стремятся объединить в единую базу данных и применять единый стандарт хранения и обработки данных.

Используются базы данных и в учебных учреждениях. Все данные учеников, учителей и сотрудников школы хранятся на локальной базе данных. Такая база используется в процессе обучения (электронные дневники, успеваемость), а также в пропускной системе, с помощью которой можно вести точную статистику посещаемости.

Базы данных и программные комплексы также активно используются в правоохранительных органах. Они имеют свою специфику. Основная задача — быстрый доступ к различным базам

данных для получения наиболее полной информации о гражданах для проведения расследований. Для этих целей также есть доступ к социальным сетям и программам для отслеживания цифровых следов, оставляемых жертвами и преступниками в интернете. Система распознавания лиц с городских систем видеонаблюдения также интегрирована в работу полиции: с их помощью можно получить информацию о местонахождении преступника или пропавшего лица и получить записи для расследования инцидентов.

Исследование показало, что интеллектуальные технологии, такие как ИИ, могут помочь городам снизить уровень преступности на 30-40 % и сократить время реагирования экстренных служб на 20-35 %. В различных странах в 84 % случаев полиция использует распознавание лиц и биометрические данные, автомобильные и нательные камеры для полиции — в 55 % случаев, беспилотники и воздушное наблюдение — в 46 % случаев, а также краудсорсинговые сообщения о преступлениях и приложения для экстренных случаев — в 39 %. Но только 8 % используют анализ больших данных и искусственный интеллект для улучшения работы полиции. По данным AI Global Surveillance (AIGS) Index 2019 только 56 стран из 176 использует искусственный интеллект для городских систем видеонаблюдения.

Городские ЦОД видеонаблюдения зачастую включают в себя школьные системы и предоставляют доступ к данным по запросу правоохранительных органов.

Некоторые системы онлайн-мониторинга поведения включают и персональные устройства ученика. Поэтому мониторинг может вестись 24/7 и при обнаружении риска сигнал поступает руководству школы и родителям. Системы родительского контроля взаимодействуют с центрами психологической помощи, с полицией, городскими службами экстренной помощи. С помощью таких систем стало возможным предотвращение рисков на ранней стадии.

Ограничения

Инфраструктура может быть подвержена хакерским атакам, что может привести к утечке персональных данных учеников и поставить под угрозу безопасность ребенка.

К ограничениям также относятся высокие технические требования к аппаратному обеспечению во всех частях инфраструктуры, необходимость в их регулярном обновлении и поддержании работоспособности.

Несмотря на то, что требуется адаптация систем инфраструктуры для нужд детей и их защиты от киберрисков, компании, которые занимаются инфраструктурой, редко учитывают детей в качестве стейкхолдеров при разработке своих проектов.

Ложноположительные результаты систем распознавания лиц неизбежны из-за того, что оценки сходства основаны на вероятности. Разработчики таких систем настраивают их на постоянное совершенствование и обучение, что с течением времени может привести к уменьшению таких результатов. Факт ложноположительного результата не означает, что технология распознавания лиц несовершенна, однако он указывает на важность установки соответствующего порога сходства и на необходимость проверки и подтверждения сходства вручную в тех случаях, когда неверная идентификация может иметь серьезные последствия, например, при расследовании правоохранительных органов.

Различные технологии слежения и биометрии зачастую негативно воспринимаются как детьми, так и родителями. Из-за этого дети могут стараться обойти и обмануть такие системы. Согласно опросу аналитического центра НАФИ, половина опрошенных граждан не поддерживает использование биометрических данных и создание единой биометрической системы.

Также остаются правовые вопросы, касающиеся сбора биометрических данных детей, их хранения, обработки и передачи третьим лицам.

Примеры

Система «Оруэлл»

Система «Оруэлл» — российская система видеонаблюдения с возможностями компьютерного зрения и видеоаналитики с функцией распознавания лиц, предназначенная для автоматического обнаружения и классификации различных ситуаций, которые могут представлять угрозу для людей.

Ntechlab

Ntechlab — компания-разработчик систем распознавания лиц. Алгоритм компании FindFace Security используется в российских школах и интегрирован в системы городского видеонаблюдения. Система распознавания лиц интегрирована с различными государственными базами данных в России.

AviaTor

AviaTor **—** инфраструктурный проект международной ассоциации горячих линий интернета INHOPE, которая объединяет 50 горячих линий в 46 странах для борьбы с материалами, содержащими сексуальное насилие над детьми. AviaTor — это система, в рамках которой модераторы обрабатывают изображения, расставляя маркеры и хеши, фиксируя их в базе. Это позволяет автоматически выявлять аналогичные преступные материалы в интернете. INHOPE передает данные правоохранительным органам, что содействует поиску и поимке преступников, распространяющих такие материалы. Также изображения детей сверяют с фотографиями из различных баз данных организаций по защите детей таких, как Национальный центр США по поиску и защите пропавших без вести и эксплуатируемых детей (NCMEC). Такие общественные инициативы и НКО проделывают неоценимую работу для безопасности детей и тесно сотрудничают с полицией и Интерполом.

AgeCertificate

AgeCertificate — решение, созданное банком Deutsche Bank в рамках проекта Deutsche Bank API Program. AgeCeritifcate помогает онлайн-продавцам взрослой продукции не допустить на свои сайты несовершеннолетних. AgeCertificate предлагает проверку, в основе которой лежат клиентские данные банка, в режиме реального времени проверенная информация о возрасте пользователя поступает на сайты. Это позволяет повысить достоверность данных о возрасте посетителей.

Источники

1. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 10.09.2021 № 930 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с

использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации»
2. Арсентьев М. «Особенности видеонаблюдения в школе с точки зрения инсталлятора», Системы безопасности #2, (2016)
3. Варавка Ю. «Обеспечение безопасности образовательного учреждения» (2009)
4. Васильева А. и др. «Контрольная по биометрии». Коммерсантъ (2021), https://www.kommersant.ru/doc/4976693
5. Головко Н. «Биометрия в России: правовое регулирование и практика применения» (2019)
6. Официальный сайт NTECH LAB, https://ntechlab.com
7. Позычанюк В. «Операция «Детские ладошки». Зачем «Сбер» собирает биометрические данные школьников». The Bell (2020), https://thebell.io/operatsiya-detskie-ladoshki-zachem-sber-sobiraet-biometricheskie-dannye-shkolnikov
8. Скобелев В., Чернышова Е. «Половина россиян не поддержали создание властями биометрической системы». РБК (2020), https://www.rbc.ru/technology_and_media/28/12/2020/5fe5cee59a7947dfd4362d12
9. Титов Алексей. «Комплексные Системы Безопасности VS Интегрированные Системы Безопасности». ИНТЕМС, (2022), securityrussia.com/blog/ksb-vs-isb.html.
10. Хрипунова М. «Антитеррористическая безопасность в школе и детском саду: как обеспечить соблюдение норм», АБиУС (2021)
11. Ястребова С. «Мэрия Москвы выбрала технологии для системы поиска и распознавания лиц». Ведомости (2020), https://www.vedomosti.ru/technology/articles/2020/01/29/821677-algoritm-opredelyaet
12. «Биометрия и стандарты. Наблюдения за развитием технологий», Новости МСЭ (2010).
13. «В московских школах установят тысячи видеокамер за миллиарды рублей». Cnews (2021), https://www.cnews.ru/news/top/2021-08-20_v_rossijskih_shkolah_ustanovyat
14. «Компрометация тела, или как утекают биометрические данные», INFOWATCH (2018), https://www.infowatch.ru/analytics/daydzhesty-i-obzory/komprometatsiya-tela-ili-kak-utekayut-biometricheskie-dannye
15. «Рекомендации по организации действий в кризисной ситуации для участников образовательных отношений». Министерство Просвещения Российской Федерации (2021)
16. «Ярославская область – территория безопасного детства». Уполномоченный по правам ребенка в Ярославской области (2020)
17. Brown M. «K–12 Leaders Weigh Threats and Benefits of Increased Web Monitoring». Technology Solutions That Drive Education (2020)
18. Herold B. «Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming». Education Week (2022)
19. Kamenetz A. «To Prevent School Shootings, Districts Are Surveilling Students' Online Lives», NPR (2019)
20. Leibowitz A. «Could Monitoring Students on Social Media Stop the Next School Shooting?» The New York Times (2018), https://www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html
21. Whyte, Jennifer. «The future of systems integration within civil infrastructure: A review and directions for research. INCOSE International Symposium» (2016)
22. Xu, J. «A deep learning approach to building an intelligent video surveillance system. Multimed Tools» Appl 80, 5495–5515 (2021)
23. Ye, Liang et al. «A Video-Based DT-SVM School Violence Detecting Algorithm». Sensors (Basel, Switzerland) vol. 20,7 (2020)
24. «AI Global Surveillance Technology». Carnegie Endowment forinternational peace

25. «Dfat child protection guidance note infrastructure activities», Department of Foreign Affairs and Trade, Australian Government. (2017)
26. «Emerging tech that can make smart cities safer: High-tech still needs to be high-touch», Deloitte (2018)
27. «Face Facts: Dispelling Common MYTHS. Associated With Facial Recognition Technology», Security Industry Association, https://www.securityindustry.org/report/face-facts-dispelling-common-myths-associated-with-facial-recognition-technology/
28. «How Software Is Taking On School Shootings». Fast Company (2018), https://www.fastcompany.com/40477172/could-software-stop-school-shootings
29. «Internet Monitoring Software to Control Cyber-bullying In Schools», PearlSoftware, https://www.pearlsoftware.com/solutions/cyberbullying-in-schools.html
30. «Orwell 2k», официальный сайт Элвис-НеоТек, www.elveesneotek.ru/products/orwell-2k.php
31. «Urban future with a purpose: 12 trends shaping human living», Deloitte (2021)

Риски в будущем

1. Инфлюенсеры, рост их влияния и виртуализация

С ролью лидеров мнений, инфлюенсеров нельзя не считаться — они влияют на мнение и выбор людей, транслируют свои ценности и пользуются доверием со стороны аудитории.

Инфлюенсеры также популярны и среди детей, которые формируют с ними парасоциальные отношения. При этом они не всегда осознают ответственность за идеи и мысли, которые транслируют своей аудитории. Более того, инфлюенсеры не всегда способны контролировать свою аудиторию. Контент, который производится инфлюенсерами в качестве шутки или сатиры, может быть вырван из контекста или воспринят ребенком серьезно. Например, шутки могут превращаться в опасные тренды и флешмобы.

Инфлюенсеры могут быть как реальными, так и полувиртуальными и даже полностью виртуальными. В качестве примера полувиртуальных инфлюенсеров можно привести витьюбера — это реальный человек, использующий виртуальный аватар для производства контента. Полувиртуальные инфлюенсеры отличаются повышенной анонимностью. А полностью виртуальные инфлюенсеры — это несуществующие персоны, которые используются группой людей или компанией для производства контента.

> **Лил Микела**
>
> Лил Микела — известный виртуальный инфлюенсер, модель и певица. У нее несколько миллионов подписчиков в Instagram*. Долгое время подписчики не подозревали, что девушка не является реальной личностью. Лил Микела ведет свой блог, публикует фото в разных одеждах, снимки с едой, увлечениями, рассказывает о своих жизненных принципах. Однако за тем, что транслирует персонаж, стоит команда разработки со своими мотивами и задачами.

Проблема ценностей, транслируемых инфлюенсерами, обостряется с усилением виртуализации, так как живая, полностью реальная медиаперсона ограничена в возможностях по созданию контента.

Негативные эффекты от парасоциальных отношений можно наблюдать уже сейчас, однако есть вероятность, что дети, выросшие в обществе, где инфлюенсеры определяют тренды и привлекают к себе все больше внимания, будут более уязвимы к этим эффектам.

Кроме того, имидж и внешний вид и виртуальных инфлюенсеров может создавать дополнительные риски для детей — идеальные пропорции тела и лица, умная ретушь и прочее функции, которые становятся возможны благодаря виртуализации, могут вызывать у детей и подростков проблемы с самооценкой.

2. Взаимодействия между взрослыми и детьми в VR и метавселенных

В современных VR-приложениях степень контроля за взаимодействием детей и взрослых низка. Взрослые могут использовать аватары детей, а дети могут использовать аватары

взрослых — это фундаментальная часть преимуществ VR-пространства и одна из ключевых форм самовыражения.

С коммодизацией VR и метавселенных все больше людей разных возрастов будут выходить на одни и те же площадки. Уже сейчас в VR существуют прецеденты кибербуллинга, сексуальных домогательств и других действий, которые способны распространить сопутствующие риски на детей и подростков.

Отдельной проблемой является то, что анонимность в VR может быть значительно выше в контексте социального взаимодействия. Программы для редактирования голоса и видео в режиме реального времени непрерывно развиваются — они станут не только совершеннее в плане качества, но и продолжат улучшать свои интерфейсы.

Сексуальное домогательство в метавселенной Meta* (2021)

В ноябре 2021 года одна из бета-тестировщиков виртуальной вселенной Meta* пожаловалась на домогательства со стороны другого игрока. Вот что она написала на форуме: «он приблизился ко мне своим аватаром и пытался потрогать меня». Согласно ее посту, помимо другого игрока, который «лапал» ее аватара в виртуальной вселенной, в локации были и другие люди, которые поддерживали такое поведение. Все это в совокупности заставило ее чувствовать себя совсем одинокой и вызвало чувство тревоги.

Барьер между ребенком и такими программами ранее состоял из повышенных требований к цифровой грамотности и техническим знаниям. Однако по мере развития подобных решений и упрощения процесса их использования, может сложиться ситуация, в которой взрослые будут общаться с детьми, не подозревая, что перед ними ребенок. Возраст акторов в этой ситуации легко будет заменить и в обратную сторону — взрослый злоумышленник, маскирующийся под ребенка с помощью аватара и программ для редактирования голоса, будет представлять повышенную опасность для детей.

3. ИИ как инструмент преступников

Коммодизация искусственного интеллекта, упрощение отладки нейросетей и выход подобных технологий на потребительский рынок позволят злоумышленникам использовать их в качестве инструмента. Так, еще в 2016 году нейросеть использовалась для доксинга актрис из эротических роликов, а исследователи безопасности в IBM Research продемонстрировали компьютерный вирус, который базируется на технологии машинного обучения.

Развитие технологий для производства дипфейков[14] продолжится, и уже сейчас есть примеры систем, способных копировать лицо, голос и мимику, — это может использоваться мошенниками для обхода систем, базирующихся на биометрической верификации. Эти же технологии позволяют агрессивно настроенному ребенку создать фото или видео, в которых сверстник находится в компрометирующей ситуации. Развитие технологий машинного обучения приведет к способности имитировать связную, осмысленную человеческую речь, что неизбежно будет использоваться в самых разных видах мошенничества, чтобы автоматизировать и масштабировать их.

[14] Дипфейк (англ. deepfake) — методика синтеза изображения, основанная на искусственном интеллекте.

4. ИИ как часть процесса воспитания

Дети впитывают информацию из окружающей среды и адаптируют ролевые модели взрослых, в том числе образ мышления. Образ мышления человека и аналогичные процессы у ИИ сильно отличаются. Когда дети начинают пользоваться голосовыми помощниками и умными устройствами с голосовым управлением в самом детстве, они могут неправильно понимать роль ИИ в их жизни.

В 2018 году в западном обществе разгорелись дебаты из-за того, что младенец сказал «Алекса» в качестве своего первого слова. Ребенок может не понимать, что робот или ИИ — это инструменты, совершенные программы, а не живые существа с самосознанием, и могут к ним привязываться.

Кроме того, домашние голосовые ассистенты открывают новый вектор для вторжения корпораций в семью. Существует вероятность, что дети, пользующиеся ИИ-ассистентами как игрушками, станут жертвами создателей таких приборов. Создатели могут транслировать через них идеи, манипулировать алгоритмами подбора контента, собирать данные. Также возникает вопрос об осознании родителями того, что корпорации начинают принимать беспрецедентную роль в воспитании их детей.

> **Смертельно опасная рекомендация умной колонки для ребенка (2021)**
>
> Сервис Alexa, встроенный в умную колонку Amazon Echo, порекомендовал десятилетней девочке опасный и потенциально смертельный способ развлечься. Девочка попросила голосового помощника подыскать ей самый популярный челлендж. «Задача проста: вставьте зарядное устройство для телефона в розетку примерно наполовину, а затем приложите монетку к открытым контактам», — порекомендовала Alexa. Данный челлендж стартовал в TikTok и набрал популярность в сети. Вовлекая всё больше детей, он был назван «ночным кошмаром школ». Также из-за возгораний, травм и негативных последствий был цитирован многими СМИ. Возможно поэтому рекомендательные алгоритмы определили данный челлендж как «популярный» по принципу цитирования.

5. Дистанционные способы эксплуатации детей

Одна из механик Web 2.0 — создание контента пользователями. Школьники уже сейчас абсолютно бесплатно производят контент на платформах коммерческих компаний. Например, сотни часов групповой работы уходят на проекты в видеоигре Roblox, прибыль за которые получает компания, а не фактические создатели контента. TikTok также очень популярен у детей и работает исключительно благодаря контенту, созданному пользователями.

Кроме того, подростки ищут подработку в интернете, где взаимоотношения работника и нанимателя контролируются слабо. Некоторые дети зарабатывают низкооплачиваемым, неэффективным трудом, при этом ненормированная подработка может наносить ущерб успеваемости. Ребенок может не осознавать, что его время более ценно, чем деньги, полученные от задач, которые он выполняет. Наконец, пытаясь найти подработку, подросток может наткнуться на мошенников.

Кроме того, часть из детей продает предметы из игр на сторонних торговых платформах. Получение игровых предметов фактически превращается в работу, которая, в свою очередь, может приводить к игровой зависимости.

Детская работа в реальной жизни регулируется законом согласно с решениями этических и медицинских комитетов. В то же время тема эксплуатации детского труда в интернете мало изучена. Взрослые редко понимают, по каким правилам функционирует экосистема виртуального труда детей.

6. Цифровой след и биометрические данные

Цифровой след начинает накапливаться ребенком с самого раннего возраста. Это является вектором для разнообразных атак: неосторожное высказывание в интернете может стать поводом для увольнения, а обширный цифровой след сам по себе — идеальная цель для сталкеров и проектов по профилированию. Дети не всегда понимают, как содержание их высказываний в интернете может сказаться на их будущем, когда они повзрослеют.

Биометрические данные — самый «персональный» вид данных, которые есть у человека. Изменить имя, адрес, IP-адрес и другие социальные координаты гораздо проще, чем изменить свое лицо, отпечатки пальцев или ДНК.

> **Гонконг и биометрические данные (2015)**
>
> В 2015 в Гонконге прошла уникальная кампания социальной рекламы: биллборды на улицах показывали лица людей, сгенерированные из их генетических данных. Сгенерированные компьютером лица были близки к фотографиям, и их предназначением было пристыдить людей, которые мусорили на улицах. Компания, которая проводила эту акцию, получила банк с ДНК из самых разных источников мусора на улицах — жвачек, бычков сигарет, стаканчиков из-под кофе.
> Эта пиар-кампания начала дискуссию об этичности сбора подобных биометрических данных.

7. Трансформация социальных навыков детей

Длительный карантин погрузил людей в массовую изоляцию. Дети также стали жертвой обстоятельств — они начали больше общаться онлайн, пользоваться домашними устройствами с ИИ и формировать парасоциальные связи с блогерами и инфлюенсерами. Процесс освоения социального поля изменился, и дети, которые сильнее полагаются на интернет, могут иметь проблемы с традиционной формой социализации.

Так как дети контактируют друг с другом онлайн, они проводят больше времени в интернете. Например, вместо спортивной площадки они встречаются в играх и развивают компетенции, отличающиеся от компетенций старшего поколения. Такая ситуация ставит их под риски в направлениях игровой зависимости и зависимости от интернета.

8. Популяризация «серых» взаимодействий

Массовые ограничения доступа к ресурсам в интернете и возможная регионализация интернета уже привели к распространению различных сервисов и подходов по преодолению вводимых запретов. Такие программы популярны и у взрослых, и у детей, имеют удобный интерфейс и часто выкладываются в интернет с руководствами по настройке.

При фрагментации и регионализации интернета проблема может значительно усугубиться, вплоть до появления особых «серых» устройств. Такое уже происходило в СССР, когда капиталистические страны вкладывались в проекты, заточенные на радиопропаганду с использованием специальных устройств. Учитывая, что на данный момент Россия испытывает затруднения с разработкой собственных компьютеров, производством полупроводников, процессоров и других важных элементов интернет-инфраструктуры, защититься от повторения такой ситуации может оказаться крайне сложно.

Попытки ограничить доступ к интернет-площадкам приводят к новой форме гражданского неповиновения — оно переходит в киберпространство. Будучи неготовым принять точку зрения государственных структур по поводу блокировки любимого интернет-ресурса, пользователь может начать сомневаться в целесообразности блокировок. В условиях ухода международных медиахолдингов из страны складывается ситуация, когда легального способа посмотреть кино или послушать музыку нет, пиратские сайты заблокированы, а отечественный рынок не способен предоставить потребителю все необходимые медиа-продукты.

Популяризация «серых» взаимодействий может привести ребенка не только к изучению информационных и коммуникационных технологий, но и к вступлению в хакерскую ячейку на роль так называемого script kiddie — юного подмастерья более опытных хакеров.

9. Ужесточение информационной войны

Разные акторы все сильнее используют киберпространство для информационных войн. Государства, корпорации, движения, политические партии и даже сообщества людей активно отстаивают свои интересы, распространяя выгодную им информацию по всем возможным каналам. При этом все стороны таких междоусобиц, включая государства и корпорации, используют всю возможную власть, чтобы бороться с неугодными точками зрения. Информационная война также ведется между акторами разных категорий: страны блокируют сайты, ИТ-компании выгоняют государственных деятелей со своих платформ. Во многих из этих конфликтов принимают участие, а также становятся жертвами дети.

Дети страдают не только от блокировок, будь то со стороны корпораций или правоохранительных органов — они нередко принимают раскрученные нарративы на веру. В результате они могут менять свои собственные позиции и проявлять активность — поддерживать свою сторону, занимать посты модераторов, создавать собственные сообщества. В контексте информационной войны все эти действия ставят детей на сторону баррикад. Но обратная сторона баррикад никогда не пуста. Санкции, применяемые к ребенку неформальными сообществами, государствами и корпорациями, не делают скидки на возраст и дальновидность ребенка.

Уже существуют примеры скандалов, когда подростков выгоняли из ВУЗов, судили, бойкотировали за что-то, что они сказали в детстве. Жесткая защита своих интересов стейкхолдерами приводит к тому, что несогласные уходят в неподконтрольные пространства, где начинает происходить радикализация. Чем глубже в такие пространства заходит ребенок, тем тяжелее ему строить стабильные социальные связи через интернет, и тем уязвимее он становится для злоумышленников. В таких подпольных киберпространствах не только увеличивается риск стать жертвой злоумышленника: обживший какое-то пространство ребенок

пользуется преимущественно им, а в подпольных пространствах детям сложнее найти защитников, консультантов и иным образом запросить помощь. Подпольные пространства будут существовать всегда, но именно за стейкхолдерами остается выбор о том, загонять ли детей в кибернетическое гетто.

Ограничение каналов информации и информационные пузыри приводят к радикализации. В определенных сообществах это вылилось в «культуру отмены» — новую форму остракизма, при которой радикально настроенные люди давят на окружающих с целью лишить своего оппонента всей возможной поддержки. Для толпы людей, которая разъярена, нет разницы между ребенком и взрослым. Сами дети также подхватывают эту тенденцию, наносят ущерб другим людям. При интенсификации информационных войн главными жертвами будут дети, и последствия будут множиться, а с усилением накала инфовойн эти последствия будет все сложнее предсказать.

10. Рост цифрового разрыва

Эпоха этики, соглашений и договоренностей прошла — компании, в том числе технологические гиганты, продемонстрировали, что готовы вовлекаться в формирование политической атмосферы в разных странах. Учитывая примеры последних лет, становится ясно, что эти компании готовы принимать самые жесткие меры по отношению к неугодным группам. Будучи транснациональными корпорациями со значительными ресурсами, некоторые компании способны протестовать против решений государств, но в межгосударственных конфликтах они принимают решения исключительно из своих интересов. Цифровые разрывы, которые и раньше являлись источником многих проблем и неравенства между разными регионами, усугубляются и будут расти. Технологии будут распространяться асинхронно, поэтому цифровые разрывы станут все более комплексными и могут приобрести резистентность к чисто регуляторным или технологическим решениям.

Это неизбежно скажется на детях и подростках: цифровое неравенство и фактическое поражение детей из отдельных стран в гражданских правах может ограничить детей в способности получить своевременную помощь, провайдеры услуг не смогут воспользоваться полным спектром мер по противодействию рискам, угрожающим детям и подросткам, а правоохранительные органы будут ограничены в инструментах расследования преступлений. Дети рискуют остаться в менее благополучном, а следовательно, более опасном обществе, в котором сложнее найти помощь, а технологические меры будут развиваться медленнее, чем подходы преступников.

Рекомендации стейкхолдерам

Проведенный анализ угроз и рисков, с которыми сталкиваются дети и подростки в процессе использования интернета, позволяет сформулировать ряд рекомендаций стейкхолдерам, в той или иной степени ответственным за реализацию технологий обеспечения безопасности в онлайн-среде. К числу таких стейкхолдеров мы относим государство, образовательные учреждения, коммерческие предприятия, родителей, некоммерческие организации (НКО) и социальных предпринимателей, а также разработчиков информационных технологий.

Важно учитывать, с одной стороны, что эффективная защита может быть достигнута при условии скоординированных и обоснованных усилий со стороны всех заинтересованных сторон процесса.

С другой стороны, мы убеждены, что ключевая роль в обеспечении интернет-безопасности заключается в содействии процессу формирования ребенка как осознанного и опытного субъекта, активно использующего цифровые ресурсы для своего развития.

Государство

Государство играет важнейшую и многоплановую роль в процессе обеспечения кибербезопасности детства и юношества.

Во-первых, оно регулирует отношения в сфере создания и использования интернет-технологий, определяя соответствующую политику.

Во-вторых, государство остается крупнейшим игроком в сегментах образования и здравоохранения, играет возрастающую роль в сегменте ИТ-разработки.

Наконец, в-третьих, государственные правоохранительные органы реализуют функцию защиты детей и подростков от преступлений, в том числе происходящих в интернете или с использованием интернета.

Мы полагаем, что именно государство должно взять на себя ведущую роль по организации и координации совместной деятельности различных стейкхолдеров, направленной на формирование интернет-среды, безопасной для детей и подростков. Поэтому необходимо расширение поддержки существующих и создание новых коммуникационных площадок, предназначенных для обсуждения проблем кибербезопасности и поиска совместных путей их решения. Обсуждение должно вестись на различных уровнях, включая международный, который особенно важен с учетом высокого уровня развития цифровых практик в ведущих цифровых экономиках мира. Развитие международного сотрудничества в данной области представляется крайне перспективным.

Проведенный анализ сложившейся ситуации, подкрепленный мнениями экспертов, позволяет сделать вывод о необходимости дополнительной организационной и финансовой поддержки институтов гражданского общества, включая некоммерческие организации и структуры социального бизнеса. Инициативы, направленные на повышение безопасности детей в интернете, должны пользоваться особой поддержкой. Реализация таких программ должна стать предметом постоянного межведомственного взаимодействия.

Необходимы государственные программы кодификации и мониторинга проблем кибербезопасности детей и подростков, а также программы поддержки междисциплинарных теоретических и прикладных исследований в данной сфере.

Законодательное регулирование персональных данных нуждается в совершенствовании в части открытости и безопасности практик, связанных с данными детей и подростков.

Цифровые права детей как частных, так и платформенных пользователей должны быть пересмотрены.

Необходима программа, направленная на поддержку цифровой социализации детей и подростков, а также повышение цифровой грамотности указанной выше социальной группы.

Обучение навыкам безопасности в интернете, контроль соответствующих знаний и умений должны быть включены в образовательные программы на всех уровнях, от начального до высшего.

Образовательные учреждения

Перед образовательными учреждениями различного уровня стоит комплексная задача, связанная одновременно с безопасным включением онлайн-технологий в учебный процесс, реализацией учебных программ и дисциплин, посвященных интернет-безопасности, а также цифровой социализации детей и подростков.

Безопасное использование интернет-технологий должно стать основополагающим принципом организации учебного процесса. Необходимо проведение комплексного анализа киберрисков, с которыми сталкиваются дети и подростки как во время пребывания в учебных учреждениях, так и подключаясь к учебному процессу дистанционно. Требуется стандартизация процессов, связанных с использованием компьютерных и интернет-технологий в образовании.

Образовательные модули по кибербезопасности и цифровой грамотности должны стать сквозным направлением в образовании детей и подростков на всех этапах обучения. Кроме того, должны быть разработаны программы повышения квалификации для специалистов, по роду деятельности связанных с киберзащитой детей и подростков (педагоги, юристы, сотрудники правоохранительных органов, психологи и т. д.).

Мы видим педагогов начальной и средней школы в качестве модераторов процесса формирования бытовой культуры безопасности использования интернета и цифровых технологий. Институт классного руководителя и школьного психолога нуждается в переосмыслении с учетом цифровизации среды, окружающей детей и подростков. Педагоги должны быть готовы помогать родителям и другим членам семей своих подопечных вырабатывать и согласовывать внутрисемейные правила и регламенты цифрового взаимодействия.

Консультации для родителей в области цифровой безопасности — необходимый элемент современного образовательного процесса. Совместными усилиями педагогов и родителей необходимо находить баланс между контролем и приватностью, при этом основной задачей должна стать реализация интернет-потребностей и интересов школьника на основе взаимоуважения, поддержки и развития самостоятельности.

Отдельной задачей, стоящей перед образовательными учреждениями, является изучение бытовой культуры в сфере детской кибербезопасности, анализ и использование лучших практик в данной области.

Коммерческие предприятия

В целом задача бизнеса в области обеспечения интернет-безопасности детей и подростков заключается в социально ответственной позиции по отношению к рискам и угрозам, возникающим по отношению к данной категории населения при разработке и реализации цифровых товаров и услуг, рассчитанных на различные целевые аудитории.

Коммерческие предприятия должны проводить этическую экспертизу распространяемого цифрового контента, элементов дизайна, пользовательских интерфейсов, внедряемых UX/UI решений и др., используя при необходимости их возрастную маркировку и инструменты ограничения доступа. Соответствующий функционал должен входить в сферу ответственности специальных сотрудников, занимающихся вопросами соблюдения требований в области кибербезопасности детей и подростков (Chief Kids Compliance Officer).

Особое внимание следует уделять разработке инициатив, направленных на поддержку и развитие сотрудничества бизнеса и других ключевых стейкхолдеров в области разработки и внедрения новых эффективных механизмов обеспечения приватности детей и подростков в онлайн-среде, с учетом изменений в Законе о персональных данных.

Родители

Родителям принадлежит ключевая роль в первичной социализации детей, организации их повседневных практик. Особенность ситуации заключается в том, что современная медиасистема трансформируется крайне динамично. Медийный опыт взросления современных родителей существенно отличается от опыта их детей, поэтому процесс передачи опыта между поколениями в данном случае не работает.

Перед родителями, таким образом, стоит непростая задача воссоздания, конструирования безопасной среды для их детей. За счет чего это возможно?

Во-первых, родителям следует интересоваться виртуальной жизнью своих детей, проявляя уважение и интерес к этой части социализации личности.

Во-вторых, следует использовать все возможности для повышения собственных компетенций в области цифровой грамотности и кибербезопасности.

В-третьих, необходимо делиться лучшими практиками организации интернет-активности детей, учитывающих баланс между их приватностью и контролем над действиями.

Наконец, в-четвертых, не стоит игнорировать доступные технологические инструменты информационной безопасности детей и подростков.

НКО и социальные предприниматели

Задача общественных организаций, так или иначе связанных с проблемами интернет-безопасности детства, заключается в инициативах, направленных на развитие данного направления, а также в координации действий различных акторов.

Во-первых, функция НКО заключается в создании и поддержке междисциплинарных дискуссионных площадок по вопросам кибербезопасности детей и подростков.

Во-вторых, НКО способны выступать в качестве центров знаний и компетенции для различных стейкхолдеров, нуждающихся в соответствующей экспертизе.

В-третьих, некоммерческие структуры должны взять на себя адресную поддержку детей и подростков, столкнувшихся с последствиями различного типа кибератак, а также нуждающихся в реабилитации и ресоциализации.

Следует отдельно отметить перспективность развития социального предпринимательства в сфере интернет-безопасности детей и подростков.

ИТ-разработчики

ИТ-разработчики являются источником профессиональных компетенций в области кибербезопасности, а также создателями продуктов, направленных на информационную защиту различных категорий населения, включая детей и подростков. В условиях динамичного развития медиасреды постоянно возникают новые риски и угрозы, что требует развития технологий защиты, новых продуктов в данной области, а также постоянного совершенствования навыков и компетенций.

Эффективная деятельность по разработке ИТ-решений, поддерживающих кибербезопасность и снижающих риски пользователей интернета, невозможна без обмена опытом, дискуссий на профессиональных и индустриальных мероприятий, в том числе международного уровня, изучения и использования зарубежного опыта, лучших практик, проектирования и формирования новых социальных практик и т. д.

Одним из наиболее перспективных направлений в данной области представляется развитие комплекса превентивных мер защиты на базе больших данных, профилирования, предиктивной аналитики и непрерывного мониторинга за счет сотрудничества со специалистами в области психологии, криминалистики и т. п.

Также следует обратить внимание на важность обеспечения экологичной разработки программных продуктов с учетом принципов и целей в области устойчивого развития ООН.

Методология

Исследование проводилось в два этапа. В рамках первого этапа мы провели кабинетное исследование, чтобы составить классификацию киберрисков для детей и подростков, отобрать те технологии и ИТ-решения, которые в принципе направлены на противодействие этим угрозам.

- Был проведен кластерный анализ на основе выборки, включающей более 21 тысяч научных статей.
- Были проанализированы более 500 источников литературы, посвященных теме безопасности несовершеннолетних в интернете.
- После первичной систематизации были выделены 23 киберриска. Объединение рисков в категории происходило на основе независимого экспертного кодирования: в работе участвовали 4 эксперта, каждый из которых создавал собственный набор категорий. После этого результаты работы каждого эксперта сравнивались с другими, и принималось решение о формировании категории и о ее названии. Расхождения обсуждались, и по каждому из них эксперты приходили к согласию.
- Для каждой категории мы сформировали описание, содержащее определение, рассказ о сути и специфике угрозы, доступную статистику и исследования, а также кейсы и примеры.
- Мы проанализировали более 300 ИТ-решений, патентов, коммерческих компаний, платформ и сервисов с точки зрения их реальной или потенциальной способности противодействовать киберрискам. В результате по той же аналитической процедуре были сформированы 8 категорий ИТ-решений.

Второй этап также строился на методологии агрегированных экспертных оценок. Цель этапа — рассортировать 23 киберриска по степени их опасности и эффективности технологических мер защиты детей от конкретного риска.

Для участия в работе были отобраны 24 эксперта — специалисты в области интернет-исследований (социологи, психологи, педагоги), кибербезопасности и ИТ-сферы. Каждому эксперту были предложены материалы — «карточки-паспортички» киберрисков и защитных ИТ-решений. Кроме того, был проведен онлайн-семинар с презентацией результатов первого этапа исследования, разбором киберрисков и заданий для экспертной работы.

Каждому эксперту предложили оценить по 10-балльной шкале:

- «Степень опасности» каждого риска: тяжесть последствий для психологического и физического здоровья ребенка, влияние на социальное благополучие, сложность реабилитации («1» — риск не опасен, «10» — риск имеет критический уровень опасности).
- «Эффективность технологий» защиты: насколько хорошо имеющиеся технологии защищают ребенка от конкретного киберриска («1» — защиты нет / технологии не эффективны / их нет; «10» — существующие технологии полностью защищают от риска).

Полученные оценки для каждого из рисков были проанализированы на сходимость. Оценивались различные варианты средних оценок (средняя арифметическая, медиана), а также статистическая вариация. В результате были выявлены случаи бимодального распределения. В основном это касалось оценок эффективности информационных технологий. Бимодальное распределение указывает на значимое расхождение мнений: часть экспертов

приписывали определенной технологии высокую способность защищать от рисков, а часть наоборот — приписывала более низкие оценки.

После завершения процедуры мы попросили некоторых экспертов прокомментировать их логику выставления оценок. Рассуждения и замечания систематизированы в отчете по результатам исследования.

Особенностью данного исследования является использование в его основе искусственного интеллекта (машинного обучения), превалирование методов автоматического количественного анализа в целях обеспечения достоверности результатов. Представленная информация и выводы получены с применением интеллектуальной аналитической системы выявления новых рынков, перспективных технологий и методов их использования TeqViser.

TeqViser – инструмент для объективного и своевременного принятия решений, который способен существенно дополнить традиционные методы оценки экономических перспектив инновационных разработок и технологических стартапов. Цифровые технологии не только существенно расширили исследуемую выборку, но и значительно сократили срок обработки исходных данных, представляя результаты и рекомендации для принятия управленческих решений. Исследование основано на анализе первичных источников, преимущественно текстовых англоязычных. Для получения структурированных данных из полученных массивов применяется машинный лингвистический анализ, а также анализ частоты упоминаний того или иного направления технологического развития и сферы его применения.

Источниками данных для исследования служат накопленные за несколько лет базы данных, которые позволяют анализировать тренды на разных этапах жизненного цикла, начиная от решения фундаментальных научных проблем и заканчивая практическим применением технологий в рыночных продуктах и решениях. В качестве исходных данных выбраны первичные не интерпретированные экспертами свидетельства развития технологий.

Об авторах и проектной группе

Борис Глазков
Вице-президент по стратегическим инициативам «Ростелекома»

Павел Красовский
Заместитель директора Центра стратегических инноваций «Ростелекома»

Руслан Юсуфов
Управляющий партнер MINDSMITH

Дарья Воронина
Старший аналитик, MINDSMITH

Иван Климов
Эксперт MINDSMITH, доцент факультета социальных наук, старший научный сотрудник Международной лаборатории прикладного сетевого анализа НИУ ВШЭ

Сергей Давыдов
Эксперт MINDSMITH, доцент Департамента социологии НИУ ВШЭ

Максим Кондратьев
Аналитик, MINDSMITH

Анастасия Тетеркина
Аналитик, MINDSMITH

Наталья Куровская
Аналитик, MINDSMITH

Алина Потулова
Аналитик, MINDSMITH

Даниил Щербаков
Младший аналитик, MINDSMITH

Татяна Громова
Ассистент проекта, MINDSMITH

Эльмира Гасанова
Редактор, MINDSMITH

Мария Плюснина
Корректор, MINDSMITH

Об Альянсе

Альянс по защите детей в цифровой среде — первое в России индустриальное объединение, направленное на создание дружелюбной, комфортной и безопасной для детей цифровой среды, способной в полной мере раскрыть творческий потенциал нового поколения. Альянс основали 1 сентября 2021 года девять крупнейших компаний России, работающих в сфере ИТ и коммуникаций: «ВымпелКом», «Газпром-Медиа Холдинг», «Лаборатория Касперского», «МегаФон», МТС, VK (ранее Mail.ru Group), «Национальная Медиа Группа», «Ростелеком» и «Яндекс».

Члены Альянса взяли на себя добровольные обязательства, призванные повышать цифровую грамотность детей, родителей и педагогов, развивать у детей навыки ответственного и безопасного поведения в интернете, демонстрировать им возможности созидательного использования цифровых технологий, формировать и продвигать позитивный и образовательный контент, разрабатывать новые подходы для защиты детей в интернете, создавать необходимые информационно-технологические решения для защиты личных данных, проактивно выявлять и удалять контент, который может причинить вред здоровью и развитию детей.

Важное направление работы Альянса — постоянный диалог с государством и международными организациями для объединения усилий по защите детей в цифровом мире. Альянс намерен стать лидером глобальной кооперации в сфере защиты детства в онлайн-среде и продвигать на международных площадках российские инициативы и подходы институтов гражданского общества, технологических- и медиакомпаний.

Подробная информация об Альянсе и его деятельности доступна на сайте: https://internetforkids.ru

Мы выражаем благодарность экспертам

Алексею Гусеву
Анастасие Старковой
Артему Калашникову
Виктору Ивановскому
Денису Батранкову
Дмитрию Мананникову
Екатерине Легостаевой
Елизавете Паршиной
Кристине Рагузовой
Марии Зеленовой
Наталии Фельдман
Наталье Лезиной
Наталье Хилимончик
Оксане Демьяненко
Оксане Разумовой
Ольге Журавской
Ольге Игнатченко
Роману Шапиро
Рустэму Хайретдинову
Семёну Рожкову
Сергею Башук
Юлиане Чепурной

Термины

1. Вайны — короткие видеоролики.
2. Глубокое обучение (англ. deep learning) — совокупность широкого семейства методов машинного обучения, основанных на имитации работы человеческого мозга в процессе обработки данных и создания паттернов, используемых для принятия решений.
3. Даркнет (DarkNet) — это «надстройка» над обычным интернетом, организованная с помощью частных сетей, в которых информация шифруется несколькими способами и используются специальные правила маршрутизации.
4. Дипфейк (англ. deepfake) — методика синтеза изображения, основанная на искусственном интеллекте.
5. Лутбокс — виртуальный предмет в компьютерных играх, при использовании которого игрок получает случайные виртуальные артефакты различной ценности и назначения, называемые добычей.
6. Постправда (англ. post-truth) — обстоятельства, при которых объективные факты являются менее значимыми при формировании общественного мнения, чем обращения к эмоциям и личным убеждениям.
7. Редирект — это перенаправление пользователя с одного URL на другой.
8. Секстинг — переписка, содержащая текст, фото или другие материалы сексуального характера.
9. Скрипт (англ. script «сценарий») — это небольшая программа, которая содержит последовательность действий, созданных для автоматического выполнения задачи.
10. Фишинг (англ. phishing от fishing «рыбная ловля, выуживание») — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.
11. FOMO — fear of missing out.
12. Free-to-play — способ распространения компьютерных игр, позволяющий пользователю играть без внесения денежных средств.
13. UI (User Interface) — пользовательский интерфейс.
14. UX (User Experience) — пользовательский опыт.

Источники

1. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 10.09.2021 № 930 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации»
2. «Рекомендации по организации действий в кризисной ситуации для участников образовательных отношений». Министерство Просвещения Российской Федерации (2021)
3. Абдулаева Асият. «Ограничения права несовершеннолетних на получение и доступ информации». Проблемы совершенствования законодательства (2020)
4. М.Хрипунова. «Антитеррористическая Безопасность в школе и детском саду: как обеспечить соблюдение норм», АБиУС (2021)
5. Авдеева Наталья и Наталья Фоминых. «Влияние телевизионной рекламы на детей и подростков» (2003)
6. Антошкина Наталия. «За домогательство в Сети — 6 лет тюрьмы. О первом приговоре интернет-маньяку». Radiovesti.ru, (2014), radiovesti.ru/brand/61178/episode/1413516.
7. Анцупов Игорь и др. «О проблемах повышения цифровой грамотности молодежи: генезис проблемы, подходы психолого-педагогической науки». Проблемы современного педагогического образования 67-4 (2020): 31-33
8. Арзуманов Илья. «Детское рабство: каждый 10-й ребенок в мире подвергается эксплуатации». Плюс один (2021), https://plus-one.ru/society/2021/07/23/detskoe-rabstvo
9. Архипова А.Д. «Предупреждение преступлений несовершеннолетних, связанных с незаконным оборотом наркотических средств». Скиф. Вопросы студенческой науки № 11 (2019)
10. Афанасьева Эльмира. «Современные тенденции развития российского рынка детских товаров». Управление экономическими системами: электронный научный журнал №2 (74) (2015)
11. Белицкий В. Ю. «Распространенные виды мошенничеств в сети интернет». Актуальные проблемы современности 2 (2020): 31-36
12. Бильгин Мехмет. «Исследование особенностей интернет-зависимости у подростков». Психология. Историко-критические обзоры и современные исследования 7.6A (2018): 175-186
13. Благовещенский Антон. «Евгений Касперский: Соцсети сыграли решающую роль в похищении сына». Российская газета (2011), rg.ru/2011/05/18/kasperskii-site-anons.html.
14. Богданова Диана. «Sharenting — родительская любовь или безответственность?» Народное образование, № 1 (1472) (2019)
15. Богданова Диана. «Информационный мир: новые игрушки». Школьные технологии № 1 (2018)
16. Борисов Евгений. «Распространение криминальной субкультуры АУЕ среди молодежи: ключевые факторы, угрозы, меры противодействия» (2020)
17. Брускин Сергей. «Модели и инструменты предиктивной аналитики для цифровой корпорации». (2017)
18. Буети Кристина и др. «Руководящие указания для отрасли по защите ребенка в онлайновой среде». ITU (2009)
19. Бураева Людмила и Залина Дадова. «О проблемах негативного влияния глобального информационного пространства на процесс становления системы ценностей молодежи». Социально-политические науки № 5 (2018)
20. Бутаев Михаил Матвеевич, Алексей Иванович Мартышкин. «Основные методы автоматической обработки и модерации текстовых данных в социальных сетях». XXI век: итоги прошлого и проблемы настоящего плюс 10.2 (2021): 30-34

21. Бухоризода Б. Р. «Социальные сети и Интернет: новая форма совершения торговли людьми». Академическая мысль 2 (7) (2019)
22. Варавка Ю. «Обеспечение безопасности образовательного учреждения» (2009)
23. Василишина Юлия. «Втягивал подростков: 20-летнего нижегородца подозревают в вербовке террористов». Комсомольская правда (2022), https://www.nnov.kp.ru/daily/27350/4531412/
24. Ястребова С. «Мэрия Москвы выбрала технологии для системы поиска и распознавания лиц». Ведомости (2020), https://www.vedomosti.ru/technology/articles/2020/01/29/821677-algoritm-opredelyaet
25. Войскунский Александр и др. «Этическая направленность подростков и молодежи в социальных сетях». Психологические исследования 7.37 (2014)
26. Воронин Михаил и Елизавета Демидова-Петрова. «Корреляция криминогенности несовершеннолетних и проявлений экстремизма в молодежной среде» (2020)
27. Гадельшин Артем и Егор Потапов. «Оружейная культура в РФ. Причины скулшутинга и пути его предотвращения». Вопросы российской юстиции 13 (2021)
28. Годик Ю. А. «Угрозы и риски безопасности детской и подростковой аудитории новых медиа» (2011)
29. Голубых Никита и Константин Потанин. «Предупреждение вовлечения несовершеннолетних в деятельность деструктивных интернет-сообществ экстремистской направленности» (2020)
30. Горяинова Н.А. и Ю.В. Чепрасова. «Формирование здорового и безопасного образа жизни несовершеннолетних с учетом негативной информации сети интернет, связанной с незаконным оборотом наркотических и психоактивных веществ». Грани педагогики безопасности (2018)
31. Гришина Нина. «Работорговля в Африке как часть международного криминала». Азия и Африка сегодня № 12 (2018)
32. Гусева Анастасия и Станислав Шемелов. «"Белят" отправили работать: суд вынес первый приговор АУЕ — подросткам из Челнов». Бизнес-online (2021), https://www.business-gazeta.ru/article/518761
33. Дамаскин О.В. и В.В. Красинский. «Криминологическая характеристика механизма вовлечения несовершеннолетних в противоправную деятельность» (2020)
34. Даревская Виктория. «Что грозит за взрыв петард в Беларуси». Минск-Новости (2020), minsknews.by/dumal-koresh-idet-napugat-hotel-a-tut-vy-chto-grozit-za-vzryv-petard-v-belarusi
35. Добринская Дарья Егоровна. «Что такое цифровое общество?». Социология науки и технологий 12.2 (2021): 112-129
36. Дозорцева Елена и Анна Медведева. «Сексуальный онлайн-груминг как объект психологического исследования» (2019)
37. Дувалина О. Н. и Е. А. Чернявская. «Феномен интернет-аддикции как одна из причин девиантного поведения подростков». Colloquium-journal. No. 6 (30). Голопристанський міськрайонний центр зайнятості (2019)
38. Емельянов Дмитрий Александрович. «Фильтрация сетевого контента в образовательных учреждениях». Педагогическое образование в России 8 (2018).
39. Жильцова Дина. «"Газовая Фея" и "Кровавая Мери": Как защитить ребенка от интернет-спама». РИАМО (2017), riamo.ru/article/199877/gazovaya-feya-i-krovavaya-meri-kak-zaschitit-rebenka-ot-internet-spama.xl
40. Арсентьев М. «Особенности видеонаблюдения в школе с точки зрения инсталлятора», Системы безопасности #2, (2016)
41. Ивасюк О.Н. и И.В. Калашников. «Криминологические особенности современной преступности несовершеннолетних» (2019)
42. Калинина Наталья. «Риски и угрозы современной интернет-среды и их профилактика среди несовершеннолетних». Всероссийский вебинар: «Профилактика суицидального поведения детей и подростков, связанного с влиянием сети Интернет» (2017)

43. Карабанова О. А. и С.В. Молчанов. Национальный психологический журнал № 3 (31) (2018)
44. Касперский Евгений. «Дети и соцсети. Проблема, которую лучше решить поздно, чем никогда». (2011), e-kaspersky.livejournal.com/64468.html.
45. Комалова Л. Р. «2015. 01. 013-015. Интернет-коммуникация с элементами речевой агрессии. (Сводный реферат)». Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 6, Языкознание: Реферативный журнал 1 (2015)
46. Васильева А. и др. «Контрольная по биометрии». Коммерсантъ (2021), https://www.kommersant.ru/doc/4976693
47. Костенко Ярослава и Елена Сидоренко. «АУЕкнулось: почему приверженцев воровской идеологии признали экстремистами». Известия (2020), https://iz.ru/1048836/iaroslava-kostenko-elena-sidorenko/aueknulos-pochemu-priverzhentcev-vorovskoi-ideologii-priznali-ekstremistami
48. Кочиобан Алина. «Негативное влияние компьютера и интернета на психику и физическое здоровье детей». International Academy Journal Web of Scholar № 1 (43) (2020)
49. Крайнов Павел. «В Уфе врачи спасли ребенка, проглотившего гидрогелевый шарик». Комсомольская правда (2018), www.ufa.kp.ru/online/news/3107418 .
50. Кузнецов Артем и Анастасия Гусева. «"Белята", "Маслята" и "48-й комплекс": как в Челнах зачищают АУЕ». Бизнес-online (2019), https://www.business-gazeta.ru/article/445025
51. Куликов Алексей. «О некоторых аспектах оперативно-розыскного противодействия колумбайну в социальных сетях». Проблемы правоохранительной деятельности № 4 (2021)
52. Лаптев Леонид и Виктор Закатов. «Социально-психологические условия эффективной профилактики наркозависимости формирующейся личности подростка». Проблемы эффективной интеграции инновационного потенциала современной науки и образования (2018)
53. Логачев А. «AdTech Market Overview» (2019)
54. Ломакин А. С. и В. В. Боровик. «Исследование влияния доступа к интернету на психику детей». Человек в цифровой реальности: технологические риски: материалы V Международной научно-практической конференции, посвященной 75-летию Победы в Великой Отечественной войне (2020)
55. Мазанов Артём. «Флешмоб: Tide Pod Challenge». TJ (2018), tjournal.ru/internet/64899-fleshmob-tide-pod-challenge
56. Мазуров Валерий и Стародубцева Мария. «Экстремизм и терроризм в киберпространстве: угрозы миру и безопасности человечества». Сборник статей по итогам III Всероссийской студенческой научно-практической очно-заочной видеоконференции (2020)
57. Макаренко В. «На смену "китам и бабочкам" пришли "лёд и соль"» Комсомольская правда. Украина (2017), https://kp.ua/incidents/579584-na-smenu-kytam-y-babochkam-pryshly-led-y-sol
58. Медведева Анна. «Реакции детей и подростков на сексуальный онлай- груминг» (2020)
59. Меренков Анатолий. «Родители и педагоги: растим ребенка вместе» (2005)
60. Мирончук Роман. «Выпейте 40 таблеток и посмотрите, что будет: в сети распространяется смертельный челлендж». РБК-Украина (2021)
61. Михайлова Е.А. «Телефоны доверия как инструмент профилактики социального неблагополучия» Мониторинг общественного мнения: экономические и социальные перемены (2013): 109-113.
62. Миюзов Роман Евгеньевич. «Применение технологии искусственного интеллекта при модерации контента в сети интернет». Студенческая наука: актуальные вопросы, достижения и инновации. 2021
63. Мусаелян Марат. «Личность участника неформальных молодежных экстремистских организаций (группировок)», Адвокат № 7 (2010)
64. Мустафина Екатерина. «Влияние рекламы на психику детей и подростков». Вопросы российской юстиции 14 (2021): 7-19

65. Мылтасова О. В. и А. А. Овсянникова. «Интернет-зависимость и влияние онлайн-игр на подростков». Современное общество: вопросы теории, методологии, методы социальных исследований (2019)
66. Научно-технический центр ФГУП «ГРЧЦ», Правовое регулирование защиты несовершеннолетних пользователей сети «Интернет» от вредоносного контента (2021), https://rdc.grfc.ru/2021/08/minors_law_protection/
67. Нашилов Егор. «Байки из Steam: как разводят геймеров». Kaspersky (2021), https://www.kaspersky.ru/blog/tales-from-steam/30090/
68. Немцева Мария. «Вооруженный глаз: как распознать дипфейк». Известия (2021), iz.ru/1137510/mariia-nemtceva/vooruzhennyi-glaz-kak-raspoznat-dipfeik
69. Никитина Ирина. «Финансовое мошенничество в сети Интернет». Вестник Томского государственного университета. № 337 (2010): 122–124.
70. Николаева Эльвира и Светлана Румянцева. «Интернет-зависимость подростков как информационно-психологическая угроза». Балканско научно обозрение 3.1 (3) (2019).
71. Новости МСЭ. «Биометрия и стандарты. Наблюдения за развитием технологий» (2010).
72. Официальный сайт «Microsoft», https://www.microsoft.com/en-us/photodna
73. Официальный сайт YouTube Kids, https://www.youtube.com/kids/
74. Панов В.П. и Х.Д. Аликперов. «Юридический словарь»
75. Пашенцев Евгений и др. «Злонамеренное использование искусственного интеллекта в Северо-Восточной Азии и угрозы международной информационно-психологической безопасности». Государственное управление. Электронный вестник 80 (2020)
76. Перевозчикова Марина и Антон Сапегин. «Способы контроля доступа школьников к компьютерным ресурсам». Концепт 10 (2014)
77. Перцева Евгения. «Опасные игры: доля некачественных детских товаров выросла вдвое». Известия (2020), iz.ru/1036122/evgeniia-pertceva/opasnye-igry-dolia-nekachestvennykh-detskikh-tovarov-vyrosla-vdvoe
78. Петров А.А. «Цифровой след человека: плюсы и минусы». Большая Евразия: Развитие, безопасность, сотрудничество 3-2 (2020): 529-542.
79. Петрова Дарья и др. «Проблемы профилактики наркозависимости среди несовершеннолетних». Человеческий капитал № 3 (2015)
80. Петросян Сильва и Гегине Хачатрян. «Торговля людьми (траффикинг)» (2013)
81. Плотников Г. И. «Система автоматической модерации текста на основе искусственных нейронных сетей». Вестник современных исследований 12.1 (2018): 641-645
82. Политика использования данных Instagram, https://help.instagram.com/519522125107875
83. Понарина М. С. и М. В. Янаева. «Основные направления поиска потенциально опасного контента в социальных сетях». Технологические инновации и научные открытия (2021)
84. Правила публикации контента Pikabu, https://pikabu.ru/information/rules
85. Прозументов Лев. «Криминологическая характеристика преступности несовершеннолетних» (2004)
86. Прокопенко Ольга и др. «Противодействие торговле людьми: правовые и экономические аспекты». Право и практика (2017)
87. Скобелев В., Чернышова Е. «Половина россиян не поддержали создание властями биометрической системы». РБК (2020), https://www.rbc.ru/technology_and_media/28/12/2020/5fe5cee59a7947dfd4362d12
88. Решетникова Мария. «Как настроить смартфон ребенка: родительский контроль и не только». РБК. Тренды (2022), https://trends.rbc.ru/trends/education/62036f839a7947d009ad568b
89. Родионова Валентина. «Курьер из Burger King домогался ребенка, пока родителей не было дома». Ридус (2020), www.ridus.ru/news/336390.
90. РОССТАТ «Численность населения Российской Федерации по полу и возрасту» (2021)
91. Рыков Валерий. «Взаимодействие государств-участников ЕС в борьбе с сексуальной эксплуатацией детей и детской порнографией» (2021)

92. Официальный сайт интернет-магазина Netpolice, https://www.netpolice.ru/
93. Официальный сайт компании Cyacomb, https://cyacomb.com/cyacomb-safety/
94. Официальный сайт компании Smart-soft, https://ti.smart-soft.ru/solutions/firewall-ngfw/
95. Официальный сайт проекта Герда Бот, https://gerdabot.ru
96. Официальный сайт сервиса Kaspersky Safe Kids, www.kaspersky.ru/safe-kids
97. Официальный сайт сервиса Lidrekon, https://lidrekon.ru/block/
98. Официальный сайт сервиса SkyDNS, https://www.skydns.ru/
99. Официальный сайт сервиса родительского контроля Bark Technologies, https://bark.us
100. Официальный сайт сервиса Яндекс.DNS https://dns.yandex.ru
101. Седых И. А. «Индустрия компьютерных игр». НИУ ВШЭ (2020)
102. Селизарова Варвара. «На что дети тратят карманные деньги». РБК +1 (2017), https://plus-one.rbc.ru/society/na-chto-deti-tratyat-karmannye-dengi
103. Сергеев Сергей. «Ивантеевский школьник получил срок за побоище». Коммерсантъ (2019), https://www.kommersant.ru/doc/3887763
104. Силуянова Юлия. «Борьба с торговлей детьми в России: поиски решения проблемы». Государственное управление. Электронный вестник № 81 (2020)
105. Силуянова Юлия. «Факторы, производство, развитие, промышленность, торговля, люди в России и в мире» (2019)
106. Скобликова Т. В. и Е. В. Скриплева. «Интернет-зависимость в молодежной среде как одна из проблем современного общества». Современные проблемы науки и образования №2 (2020)
107. Смирнов А. А. «Глубокие фейки. Сущность и оценка потенциального влияния на национальную безопасность». Свободная мысль 5 (1677) (2019): 63-84
108. Смирнов Игорь. «Не надо разбрасываться своими персональными данными». Психология и педагогика служебной деятельности № 4 (2020)
109. Смыслова Вера. «Вовлечение молодежи в социальную практику и активную общественную деятельность как одно из направлений противодействия проявлениям молодежного экстремизма в условиях радикализации и роста протестной активности» (2017)
110. Соболева А.Н. «Риски интернет-пространства для здоровья подростков: возрастной и гендерный анализ». АНО «ЦНПРО», № 1 (2016)
111. Солдатова Г. В. и др. «Пойманные одной сетью». Социально-психологическое исследование восприятия интернета детьми и подростками–М (2011)
112. Солдатова Г. У. и др. «Мы в ответе за цифровой мир: Профилактика деструктивного поведения подростков и молодежи в Интернете» (2019)
113. Солдатова Г. У. и др. «Дети России онлайн: риски и безопасность. Результаты международного проекта EU Kids Online II в России» (2012)
114. Солдатова Г. У. и др. «Цифровое поколение России: компетентность и безопасность». Litres (2020)
115. Солдатова Г. У. и др. «Эволюция онлайн-рисков: итоги пятилетней работы линии помощи “Дети онлайн”». Консультативная психология и психотерапия 23.3 (2015): 50-66.
116. Солдатова Г. У. и Теславская О. И. «Отношение к приватности и защита персональных данных: вопросы безопасности российских детей и подростков». Национальный психологический журнал № 3 (19) (2015)
117. Солдатова Галина и Теславская О. И. «Персональные данные и дети: вопросы безопасности». Эпоха науки № 12 (2017)
118. Соловьев В. С. «Мошеннические действия в социальном сегменте сети Интернет (криминологическое исследование по результатам интернет-опроса пользователей)». Известия Юго-Западного государственного университета. Серия: История и право 8.3 (2018): 100-108.
119. Соловьева Е.Н. «Интернет-зависимость в практике детского психотерапевта». Научное обозрение. Медицинские науки № 4 (2016)
120. Справка Google о вредоносном и нежелательном ПО, https://developers.google.com/search/docs/advanced/security/malware?hl=ru

121. Справка о небезопасных сайтах Mail.ru, https://help.mail.ru/atom/safety/safe_browsing
122. Справка Роскачества о родительском контроле (2020), https://rskrf.ru/ratings/tekhnologii/mobilnye-prilozheniya/roditelskiy-kontrol/
123. Тарасов Алексей. «Страна из трех букв». Новая газета (2020), https://novayagazeta.ru/articles/2017/06/16/72816-strana-iz-treh-bukv
124. Тарасова Н. В., И. П. Пастухова и С. Г. Чигрина. «Индивидуальная программа развития и система наставничества как инструменты наращивания профессиональных компетенций педагогов. Рекомендации для руководящих и педагогических работников общеобразовательных организаций» (2020)
125. Тимошина Елена. «Деструктивные субкультуры несовершеннолетних как условия их виктимизации и криминализации» (2021)
126. Титов Алексей. «Комплексные Системы Безопасности VS Интегрированные Системы Безопасности». ИНТЕМС, (2022), securityrussia.com/blog/ksb-vs-isb.html.
127. Токарев Н. В. «Использование психологического воздействия при совершении мошенничества в условиях цифровизации экономики». Молодежная наука: тенденции развития № 1 (2021): 48-52
128. Толоконникова А. В. «Безопасность детей в интернете: основные сферы сетевого регулирования и саморегулирования». И безопасность детей (2018): 70
129. Хатуев В. Б. «История становления и развития российского уголовного законодательства об ответственности за склонение к самоубийству и содействие ему». Вестник Московского университета. Серия 11. Право 4 (2018)
130. Чурилов Сергей и др. «К вопросу об информационной безопасности подростков в социальных сетях и сети интернет». Формирование гражданской устойчивости как фактор противодействия идеологии экстремизма и терроризма (2017)
131. Шевченко Марина. «Смертельные селфи: почему дети рискуют жизнью ради лайков». Vesti.ua (2018), vesti.ua/lite/health/300938-smertelnye-selfi-pochemu-deti-riskujut-zhiznju-radi-lajkov
132. Шеллер Игорь. «Darknet — темная сторона интернета». Наука через призму времени (2018)
133. Шимаев Роман. «Во время заседания: фигуранты дела "Нового величия" порезали себе руки в суде». Russia Today (2019), https://russian.rt.com/russia/article/678017-novoe-velichie-incident-sud-advokaty
134. Шкор О. Н. и А. И. Головач. «Предсказательная аналитика в маркетинге» (2021)
135. Шляпникова Ольга и Николай Паршин. «Влияние интернета на формирование противоправного поведения в подростково-молодежной среде» (2021)
136. Эяль Нир и Райан Хувер. «Покупатель на крючке». Руководство по созданию продуктов, формирующих привычки (2014)
137. Юрченко О. В. и Н. Ф. Дианова. «Проблема интернет зависимости у подростка». Вестник современных исследований 12.8 (2018)
138. Якунин Иван. «Каршеринг оказался доступным для "водителей" без прав». Коммерсантъ (2018), https://www.kommersant.ru/doc/3516138
139. Головко Н. «Биометрия в России: правовое регулирование и практика применения» (2019)
140. Официальный сайт NTECH LAB, https://ntechlab.com
141. Позычанюк В. «Операция «Детские ладошки». Зачем «Сбер» собирает биометрические данные школьников». The Bell (2020), https://thebell.io/operatsiya-detskie-ladoshki-zachem-sber-sobiraet-biometricheskie-dannye-shkolnikov
142. «Арестован 18-летний москвич, угрожавший напасть на школу». Интерфакс (2021), https://www.interfax.ru/russia/808422
143. «Борьба с дезинформацией: укрепление цифровой устойчивости Североатлантического союза», Johns Hopkins University, Imperial College London & Georgia Institute of Technology, NATO REVIEW (2021)

144. «В Девоне подросток покупал наркотики за биткоин». MyCrypter (2021), https://mycrypter.com/v-devon-podrostok-pokupal-narkotiki-za-bitkoin/
145. «В Красноярском крае троих подростков обвиняют по статье об участии в террористическом сообществе». ОВД-Инфо (2020), https://ovd.news/express-news/2020/11/21/v-krasnoyarskom-krae-troih-podrostkov-obvinyayut-po-state-ob-uchastii-v
146. «В Подмосковье курьер ресторана приставал к 11-летней девочке». Vesti.ru (2020), www.vesti.ru/article/2456881
147. «В Твери тренера осудили на пять лет за детскую порнографию». Вести. Тверь (2022), https://vesti-tver.ru/dailynews/v-tveri-trenera-osudili-na-pyat-let-za-detskuyu-pornografiyu/
148. «Вместе за лучший Интернет: библиотеки, обслуживающие детей и их партнеры». Всероссийская видеоконференция (2019)
149. «Врачи Филатовской больницы борются за жизнь годовалой девочки». «Вести», Россия 1 (2018), filatovmos.ru/feedback2/14-news/312-shariki.html
150. «Детский Рунет». Институт исследований интернета (2019), www.internetinstitute.ru/portfolio/analytics/detskiy-runet-2019-otraslevoy-doklad/
151. «Доигрались. Почему российские власти решили ужесточить контроль за лизунами, спиннерами и другими игрушками». Известия (2018), https://iz.ru/727444/ekaterina-korinenko/doigralis
152. «Доклад ООН: пандемия усугубила угрозу торговли людьми, особенно для женщин и девочек». Русская служба новостей ООН (2020)
153. «Жертва МОМО — в Киеве школьница пыталась покончить собой в День знаний». Vesti (2018), vesti.ua/kiev/301345-zhertva-momo-v-kieve-shkolnitsa-pytalas-pokonchit-soboj-v-den-znanij
154. «За 2019 год на детский телефон доверия позвонили почти 900 тыс. раз». Агентство социальной информации, (2020), www.asi.org.ru/news/2020/02/05/za-2019-god-na-detskij-telefon-doveriya-pozvonili-pochti-900-tys-raz.
155. «Использование средств родительского контроля на iPhone, iPad и iPod touch ребенка». Служба поддержки Apple, https://support.apple.com/ru-ru/HT201304
156. «Исследование функциональности наиболее популярных мобильных приложений для родительского контроля для платформ iOS и Android». Центр цифровой экспертизы Роскачества
157. «Каждый десятый школьник сообщал данные банковской карты незнакомцам». РИА Новости (2021), https://ria.ru/20210515/karty-1732410828.html
158. «Как TikTok ограничивает доступ на платформу для пользователей младше 13 лет». Правила безопасности TikTok, https://newsroom.tiktok.com/ru-ru/how-tiktok-prevents-using-the-platfrom-by-minor-users
159. «Как настроить родительский контроль на консолях PS4». Служба поддержки PlayStation, www.playstation.com/ru-ru/support/account/ps4-parental-controls-and-spending-limits/
160. «Как управлять временем использования устройств и приложений». Служба поддержки Google, https://support.google.com/families/answer/7103340?hl=ru
161. «Комплексная программа профилактики деструктивного поведения в интернете у подростков и молодежи». Фонд развития интернета и Московский институт психоанализа (2019)
162. «Компрометация тела, или как утекают биометрические данные», INFOWATCH (2018), https://www.infowatch.ru/analytics/daydzhesty-i-obzory/komprometatsiya-tela-ili-kak-utekayut-biometricheskie-dannye
163. «Мам, не публикуй мои фотографии у себя в соцсетях!». Что такое «шерентинг?» BBC News Русская служба (2019), www.bbc.com/russian/features-47731823
164. «Монетизация страха и ненависти: в России хотят запретить треш-тримы». ТВЦ (2021), https://www.tvc.ru/news/show/id/219056
165. «Мошенничество в играх во время пандемии коронавируса: как защитить себя и свою семью». Kaspersky, https://www.kaspersky.ru/resource-center/threats/coronavirus-gaming-scams

166. «На что способны Big Data или супер-кейс сети Target». Retail.ru (2015), https://www.retail.ru/cases/na-chto-sposobny-big-data-ili-super-keys-seti-target/
167. «Новое поколение интернет-пользователей: исследование привычек и поведения российской молодежи онлайн». Google and Ipsos (2017)
168. «Новое поколение: исследование детей и подростков». Ipsos (2020)
169. «Новосибирский фотограф в конспиративной квартире снимал и насиловал школьниц — чтобы задержать преступника, понадобилась помощь Интерпола». NGS.ru (2014), https://ngs.ru/text/gorod/2014/02/19/1674228/
170. «Обещание лучшей жизни. Как дети попадают в секс-рабство». Утопия (2020), https://clck.ru/ehZiH
171. «Обзор перспектив блокировки интернет-контента». ISOS, Internet Society (2017)
172. «Подражательницы хабаровских живодерок имитировали истязания над котенком ради внимания». Комсомольская правда (2016), https://www.hab.kp.ru/daily/26614/3631208/
173. «Пятилетняя девочка хотела стать феей Винкс и подожгла себя». Служба новостей pg12.ru (2016), https://pg12.ru/news/23574
174. «Рекомендация CM/Rec 13 Комитета министров странам-членам по вопросам защиты частных лиц в связи с автоматизированной обработкой персональных данных в контексте профилирования граждан» (2010)
175. «Российский школьник потратил сотни тысяч родительских денег на игру». CNews.ru (2020), www.cnews.ru/news/top/2020-12-01_rossijskij_shkolnik_potratil .
176. «Серджиу Руссу: "Жертвы торговли людьми не всегда понимают, что они жертвы"». Forbes.kz (2021), https://forbes.kz/process/serdjiu_russu_jertvyi_torgovli_lyudmi_ne_vsegda_ponimayut_chto_oni_mogut_rasschityivat_na_pomosch/
177. «Экранное Время в жизни школьника». ФБУЗ “Центр гигиенического образования населения” (2021), http://cgon.rospotrebnadzor.ru/content/62/4107
178. «Ярославская область – территория безопасного детства». Уполномоченный по правам ребенка в Ярославской области (2020)
179. «TikTok публикует результаты глобального исследования об онлайн-челленджах и их влиянии на подростков». TikTok (2021), https://newsroom.tiktok.com/ru-ru/dangerous-challenges-and-hoaxes-report-2021-russia
180. «Orwell 2k», официальный сайт Элвис-НеоТек, www.elveesneotek.ru/products/orwell-2k.php
181. «AI Global Surveillance Technology». Carnegie Endowment forinternational peace
182. «Dove Detoxify Survey». Dove (2021)
183. «Emerging tech that can make smart cities safer: High-tech still needs to be high-touch», Deloitte (2018)
184. «How Software Is Taking On School Shootings». Fast Company (2018), https://www.fastcompany.com/40477172/could-software-stop-school-shootings
185. «Internet Monitoring Software to Control Cyber-bullying In Schools», PearlSoftware, https://www.pearlsoftware.com/solutions/cyberbullying-in-schools.html
186. «Urban future with a purpose: 12 trends shaping human living», Deloitte (2021)
187. «В московских школах установят тысячи видеокамер за миллиарды рублей». Cnews (2021), https://www.cnews.ru/news/top/2021-08-20_v_rossijskih_shkolah_ustanovyat
188. A.Leibowitz. «Could Monitoring Students on Social Media Stop the Next School Shooting?» The New York Times, 6 Sept. (2018)
189. Abarca-Gómez et al. «Worldwide trends in body-mass index, underweight, overweight, and obesity from 1975 to 2016» (2017)
190. Acquadro Maran, Daniela, et al. «Health care professionals as victims of stalking: characteristics of the stalking behavior, consequences, and motivation in Italy» (2017)
191. Adair, Cam. «How to Beat Your World of Warcraft Addiction». Game Quitters (2021), gamequitters.com/world-of-warcraft-addiction

192. Ahern, Kathy. «Institutional betrayal and gaslighting». The Journal of perinatal & neonatal nursing 32.1 (2018): 59-65.
193. Ahmad, A., et al. «Parental Sensitivity and Their Awareness on a Child Sexual Harassment» (2019)
194. Al-Garadi, Mohammed Ali, et al. «Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithms: Review of Literature and Open Challenges». IEEE Access vol. 7 (2019)
195. Alter, Adam. «Irresistible: The rise of addictive technology and the business of keeping us hooked». Penguin (2017)
196. Anderson, B. and M. A. Wood. «Doxxing: A Scoping Review and Typology».
197. Anderson, Jenny. «American Kids' Daily Mobile Screen Time Is Almost 10 Times Higher than It Was in 2011» (2017)
198. App, Annie. «The State of Mobile in 2022: How to Succeed in a Mobile-First World As Consumers Spend 3.8 Trillion Hours on Mobile Devices». Report (2021)
199. Archer, Catherine. «How Influencer "Mumpreneur" Bloggers and "Everyday" Mums FramePresenting Their Children Online». Media International Australia, vol. 170, no. 1 (2019)
200. Ashton, Sally-Ann and Anna Bussu. «Peer groups, street gangs and organised crime in the narratives of adolescent male offenders» (2020)
201. Asniar and Kridanto Surendro. «Predictive Analytics for Predicting Customer Behavior». International Conference of Artificial Intelligence and Information Technology (2019)
202. Atherton, Rachel Rose. «The Nutmeg Challenge: a dangerous social media trend». Archives of disease in childhood 106.5 (2021)
203. Ayenigbara, I. «Gaming Disorder and Effects of Gaming on Health: An Overview» (2018)
204. Azcona, David, et al. «Detecting students-at-risk in computer programming classes with learning analytics from students' digital footprints» (2019)
205. Babchishin, K., et al. «The characteristics of online sex offenders: a meta-analysis» (2011)
206. Babchishin, Kelly M., et al. «Online Child Pornography Offenders are Different: A Meta-analysis of the Characteristics of Online and Offline Sex Offenders Against Children» (2015)
207. Badillo-Urquiola, et al. «Stranger Danger! Social Media App Features Co-designed with Children to Keep them Safe Online». Association for Computing Machinery (2019)
208. Barbera, P. et al. «Tweeting From Left to Right: Is Online Political Communication More Than an Echo Chamber?» (2015)
209. Baron, R.A. «The aggression-inhibiting influence of heightened sexual arousal». Journal of Personality and Social Psychology № 30 (1974)
210. Batt, Simon. «The Dangers of Shortened Links and How to Stay Safe». MakeTechEasier (2017), https://www.maketecheasier.com/dangers-of-shortened-links-and-stay-safe/
211. Begotti, Tatiana and Daniela Acquadro Maran. «Characteristics of Cyberstalking Behavior, Consequences, and Coping Strategies: A Cross- Sectional Study in a Sample of Italian University Students» (2019)
212. Bennett, D., et al. «College students' electronic victimization in friendships and dating relationships: Anticipated distress and associations with risky behaviors» (2011)
213. Berson, I.R. «Grooming cybervictims: The psychosocial effects of online exploitation for youth» (2003)
214. Beyens, Ine, et al. «I don't want to miss a thing: Adolescents' fear of missing out and its relationship to adolescents' social needs, Facebook use, and Facebook related stress». Computers in Human Behavior 64 (2016)
215. Bhabha, Jacqueline. «The child—what sort of human?». PMLA/Publications of the Modern Language Association of America 121.5 (2006): 1526-1535.
216. Bin Morshed, Mehrab, et al. «Measuring Self-Esteem with Passive Sensing» (2020)
217. Black, P.J., et al. «A linguistic analysis of grooming strategies of online child sex offenders: implications for understanding of predatory sexual behavior in an increasingly computer-mediated world» (2015)

218. Blaine, R., et al. «Promoting Sleep and Balanced Screen Time among School-Aged Children with Neurodevelopmental and Mental Health Disorders: A Parent Perspective» (2021)
219. Bloemen, Noor and David De Coninck. «Social Media and Fear of Missing Out in Adolescents: The Role of Family Characteristics». Social Media and Society 6.4 (2020)
220. Blum-Ross, Alicia and Sonia Livingstone. ««Sharenting», parent blogging, and the boundaries of the digital self». Popular Communication 15.2 (2017): 110-125
221. Bozdag, Engin. «Bias in algorithmic filtering and personalization» (2013)
222. Bradshaw, Bailey and Howard. «Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation». University of Oxford (2021)
223. Bridges, A. J., et al. «Sexual Scripts and the Sexual Behavior of Men and Women Who Use Pornography. Sexualization, Media, and Society» (2016)
224. Brion-Meisels G., et al. «Exploring effective prevention education responses to dangerous online challenges». (2021)
225. Brosch, Anna. «When the Child Is Born into the Internet: Sharenting as a Growing Trend amongParents on Facebook». The New Educational Review, vol. 43, no. 1 (2016): 225–235
226. Brown M. «K–12 Leaders Weigh Threats and Benefits of Increased Web Monitoring». Technology Solutions That Drive Education (2020)
227. Brown, Marquita. «K-12 leaders weigh threats and benefits of increased web monitoring». EdTech Magazine (2019)
228. Brunick, Kaitlin L., et al. «Children's future parasocial relationships with media characters: The age of intelligent characters». Journal of Children and Media 10.2 (2016): 181-190
229. Buchanan, L. «Advanced Marketing Strategies to Add Value to Your Business» (2021)
230. Buchanan, N. and A. Mahoney. «Development of a scale measuring online sexual harassment: Examining gender differences and the emotional impact of sexual harassment victimization online» (2021)
231. Burlock, A. and T. Hudon. «Women and men who experienced cyberstalking in Canada». (2014)
232. Burnap, Pete, et al. «Multi-class machine classification of suicide-related communication on Twitter». Online social networks and media 2 (2017)
233. Burns, By Judith. «Fake News Harms Children's Self-Esteem and Trust, Say MPs». BBC News (2018)
234. Calderoni, Francesco. «Social Network Analysis of Organized Criminal Groups. Encyclopedia of Criminology and Criminal Justice» (2014)
235. Camber, Rebecca. «Global crackdown on hackers: British teen arrested along with 14 suspected members of «Anonymous» group». Daily Mail (2010), https://www.dailymail.co.uk/news/article-2016451/Anonymous-hackers-arrested-15-suspected-members-total-including-British-teen.html
236. Campana, Mario, et al. «#dadtribe: Performing Sharenting Labour to Commercialise InvolvedFatherhood». Journal of Macromarketing, vol. 40, no. 4, (2020): 475–491
237. Cano, A. and K. D. O'Leary. «Infidelity and separations precipitate major depressive episodes and symptoms of nonspecific depression and anxiety» (2000)
238. Cantor, D., et al. «Report on the AAU campus climate survey on sexual assault and misconduct» (2020)
239. Chen, Xinran, et al. «Why Students Share Misinformation on Social Media: Motivation, gender, and study-level differences». Journal of Academic Librarianship.
240. Cheng, Yu-Shian, et al. «Internet addiction and its relationship with suicidal behaviors: a meta-analysis of multinational observational studies». The Journal of clinical psychiatry 79.4 (2018)
241. Cherry, Kendra. «What is operant conditioning and how does it work?» How reinforcement and punishment modify behavior. Verywell Mind (2019), https://www.simplypsychology.org/operant-conditioning.html
242. Child Helpline International, https://www.childhelplineinternational.org

243. Cho, Charles H., et al. «Astroturfing Global Warming: It Isn't Always Greener on the Other Side of the Fence» (2011)
244. Cho, Jaeho et al. «Do Search Algorithms Endanger Democracy? An Experimental Investigation of Algorithm Effects on Political Polarization» (2020)
245. Chun, J., et al. «An international systematic review of cyberbullying measurements» (2020)
246. Chung, Grace and Sara M. Grimes. «Data Mining the Kids: Surveillance and Market Research strategies in children's online games» (2005)
247. Clark, Lynn Schofield. «The Parent App: Understanding Families in the Digital Age». European Journal of Communication (2013)
248. Copp, J., et al. «Online sexual harassment and cyberbullying in a nationally representative sample of teens: Prevalence, predictors, and consequences» (2021)
249. Coughlan, By Sean. «"Sharenting" Puts Young at Risk of Online Fraud». BBC News (2018), www.bbc.com/news/education-4415375
250. Coughlan, Sean. «Safer Internet Day: Young ignore social age limit». BBC (2016), https://www.bbc.com/news/education-35524429
251. Coulson, Josh. «Just 26 % of EA's Revenue Now Comes From Game Sales». The Gamer (2021), https://www.thegamer.com/26-ea-revenue-game-sales/
252. Coxner, M. and Narva Jacobsson, S. «Parental privacy invasions and adolescent depressive symptoms». Orebro University (2018)
253. Crone, Eveline A. and Elly A. Konijn. «Media use and brain development during adolescence». Nature communications 9.1 (2018)
254. D Haenens, Leen, et al. «How to cope and build online resilience?» (2013)
255. Del Vicario, Michela, et al. «Echo chambers: Emotional contagion and group polarization on facebook». Scientific reports 6.1 (2016)
256. Department of Foreign Affairs and Trade, Australian Government. «Dfat child protection guidance note infrastructure activities» (2017)
257. Dhir, A., et al. «The dark side of social media: Stalking, online self-disclosure and problematic sleep» (2021)
258. Di Geronimo, Linda, et al. «UI dark patterns and where to find them: a study on mobile applications and user perception». Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (2020)
259. Directive 2011/92/EU of the European Parliament and of the council
260. Dogan, Huseyin, et al. «Perceived Parenting Styles as Predictor of Internet Addiction in Adolescence». International Journal of Research in Education and Science (2015)
261. Douglas, David M. «Doxing: a conceptual analysis» (2016)
262. Drake, Brett, et al. «A Practical Framework for Considering the Use of Predictive Risk Modeling in Child Welfare». The ANNALS of the American Academy of Political and Social Science, vol. 692, no.1 (2020)
263. Drouin, Michelle, et al. «Predicting Recidivism Among Internet Child Sex Sting Offenders Using Psychological Language Analysis». Cyberpsychol Behav Soc Netw (2018)
264. Dubicka, Bernadka, et al. «Screen time, social media and developing brains: a cause for good or corrupting young minds?» Child and Adolescent Mental Health 24.3 (2019)
265. Dunckley, Victoria L. «How the Tech Industry Uses Psychology to Hook Children». Psychology Today (2018), www.psychologytoday.com/us/blog/mental-wealth/201810/how-the-tech-industry-uses-psychology-hook-children
266. EAB «Pros and cons of virtual mental health services according to experts»
267. Edwards, Haley Sweetland. «You're addicted to your smartphone. This company thinks it can change it». Time (2018), https://time.com/5237434/youre-addicted-to-your-smartphone-this-company-thinks-it-can-change-that/

268. Egan, V., et al. «Sexual Offenders Against Children: The Influence of Personality and Obsessionality on Cognitive Distortions» (2005)
269. Ehrenberg, Alexandra, et al. «Personality and self esteem as predictors of young people's technology use». CyberPsychology, & Behavior, 11 (2008)
270. Englander, E., et al. «Defining Cyberbullying» (2017)
271. Ensign, Danielle, et al. «Runaway feedback loops in predictive policing». Conference on Fairness, Accountability and Transparency (2018)
272. eSafety Commissioner. «State of Play – youth, kids and digital dangers» (2018)
273. Falk, Emily and Christin Scholz. «Persuasion, influence, and value: Perspectives from communication and social neuroscience». Annual review of psychology 69 (2018)
274. Farsi, Maryam, et al. «Crime Data Mining, Threat Analysis and Prediction». Jahankhani H. (eds) Cyber Criminology. Advanced Sciences and Technologies for Security Applications (2018)
275. Feal Fajardo, Alvaro. «Study on privacy of parental control mobile applications». IMDEA Software Institute (2017)
276. Feal, Alvaro. «Angel or devil? A privacy study of mobile parental control apps». Proceedings on privacy enhancing technologies (2020)
277. Feldman, S. «Digital Advertisers Increasingly Target Kids» (2019)
278. Ferster, Charles B. and Burrhus Frederic Skinner. «Schedules of reinforcement». (1957)
279. Fox, Alexa K. and Mariea Grubbs Hoy. «Smart Devices, Smart Decisions? Implications ofParents' Sharenting for Children's Online Privacy: An Investigation of Mothers». Journal of Public Policy & Marketing, vol. 38, no. 4, (2019): 414–432
280. Frison, Eline and Steven Eggermont. «Browsing, posting, and liking on Instagram: The reciprocal relationships between different types of Instagram use and adolescents' depressed mood». Cyberpsychology, Behavior, and Social Networking 20.10 (2017)
281. Garvey,Marianne. «Conan OBriens tweet prompts FDA to discourage #MilkCrateChallenge». CNN
(2021), https://edition.cnn.com/2021/08/24/entertainment/milk-crate-challenge-fda-trnd/index.html
282. Ghosh, Arup Kumar. et al. «Safety vs. surveillance: what children have to say about mobile apps for parental control». Univercity of Central Florida,
www.eecs.ucf.edu/~jjl/pubs/pn1838-ghoshA.pdf
283. Giannakopoulos, Theodoros. «Violence Content Classification Using Audio Features»
(2006) Huesmann, Rowell. L. «The Impact of Electronic Media Violence: Scientific Theory and Research» (2007)
284. Gogus, Aytac and Yücel Saygın. «Privacy perception and information technology utilization of high school students». Heliyon № 5.5 (2019)
285. Gordon, Lauren. «Moms Need to Warn Their Daughters About the Silhouette Challenge». Cafemom (2021),
cafemom.com/parenting/silhouette-challenge/on-youtube-there-are-still-currently-dozens-of-tutorials-on-how-to-remove
286. Grant, K. «Child identity theft is a growing and expensive problem». CNBC (2018),
https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html
287. Gretzel, Ulrike and Daniel R. Fesenmaier. «Persuasion in recommender systems». International Journal of Electronic Commerce 11.2 (2006).
288. Guerra, C., et al. «Online sexual harassment and depression in Chilean adolescents: Variations based on gender and age of the offenders» (2021)
289. Hahn, Jason Duaine. «10-Year-Old Girl Dies Trying "Blackout Challenge" from Social Media, Mom Says». PEOPLE (2021),
people.com/human-interest/10-year-old-girl-dies-trying-blackout-challenge-from-tiktok
290. Hall, R. «A Profile of Pedophilia: Definition, Characteristics of Offenders, Recidivism, Treatment Outcomes, and Forensic Issues» (2007)
291. Hamm, M., et al. «Prevalence and Effect of Cyberbullying on Children and Young People» (2015)

292. Hawk, Skyler, et al. «Adolescents' perceptions of privacy invasion in reaction to parental solicitation and control». The Journal of Early Adolescence 28 (4) (2008)
293. He, Qinghua, et al. «Brain anatomy alterations associated with Social Networking Site addiction». (2017)
294. Heilweil, Rebecca. «Algorithms and Bias, Explained». Vox (2020),
295. Heirman, Wannes and Michel Walrave. «Predicting adolescent perpetration in cyberbullying: An application of the theory of planned behavior». Psicothema 24.4 (2012)
296. Hernández, Montserrat Peris, et al. «The risk of sexual-erotic online behavior in adolescents – Which personality factors predict sexting and grooming victimization?» Computers in Human Behavior, Volume 114 (2021)
297. Hermida, Martin and Sara Signer. «How parents accompany their children on the Internet» (2013)
298. Hermida, Martin. «Schweizer Kinder und Jugendliche im Internet: Risikoerfahrungen und Umgang mit Risiken». EU Kids Online: Schweiz (2013)
299. Herold B. «Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming». Education Week (2022)
300. Hinduja, S. and J. Patchin. «Summary of Our Cyberbullying Research (2007-2019)» (2019)
301. Hollingshead, Todd. «BYU algorithm accurately predicts when teens likely to have suicidal thoughts, behavior». BYU (2021),
https://news.byu.edu/intellect/byu-algorithm-accurately-predicts-when-teens-likely-to-have-suicidal-thoughts-behavior
302. Howard, Philip N., et al. «Digital misinformation/disinformation and children». UNICEF (2021)
303. ICO PIA Handbook (2007)
304. Jacobs, DF. «Juvenile gambling in North America: An analysis of long term trends and future prospects». J Gambl Stud. (2000): 119–152
305. Jarman, Jeffrey W. «Influence of Political Affiliation and Criticism on the Effectiveness of Political Fact-Checking» (2016)
306. Jenkins, P. «Beyond Tolerance: Child Pornography on the Internet». New York: New York University Press (2001)
307. Jochen, Peter and Patti M. Valkenburg. «Adolescents' Exposure to Sexually Explicit Online Material and Recreational Attitudes Toward Sex» (2006)
308. Jochen, Peter and Patti M. Valkenburg. «Does exposure to sexually explicit Internet material increase body dissatisfaction? A longitudinal study» (2014)
309. Joergensen, Anne Cathrine, et al. «Spinal pain in pre-adolescence and the relation with screen time and physical activity behavior». BMC musculoskeletal disorders 22.1 (2021)
310. Johannesen, Richard L, et al. «Ethics in Human Communication». Waveland Press (2008)
311. Jones, Lisa M., et al. «Trends in Youth Internet Victimization: Findings from Three Youth Internet Safety Surveys 2000-2010» (2011)
312. Jourová, V. «The impact of online marketing on children's behaviour». European Commission (2016)
313. Kahneman, Daniel. «Thinking, fast and slow». Macmillan (2011)
314. Kaluža, Jernej. «Habitual Generation of Filter Bubbles: Why is Algorithmic Personalisation Problematic for the Democratic Public Sphere?» (2021)
315. Kamenetz A. «To Prevent School Shootings, Districts Are Surveilling Students' Online Lives», NPR (2019)
316. Kamenetz, Anya. «To prevent school shootings, districts are surveilling students' Online Lives». NPR (2019),
www.npr.org/2019/09/12/752341188/when-school-safety-becomes-school-surveillance
317. Katz, Sherri Jean, et al. «Predicting Parent-Child Differences in Perceptions of How Children Use the Internet for Help With Homework, Identity Development, and Health Information» (2015)
318. Keller, Daphne. «Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling». GRUR International 69.6 (2020)

319. Keller, Franziska B., et al. «Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign» (2019)
320. Kelly, Heather. «What parents need to know about social media for kids». The Washington Post (2021), https://www.washingtonpost.com/technology/2021/03/24/instagram-kids-faq/
321. Kertysova, Katarina. «Artificial intelligence and disinformation: How AI changes the way disinformation is produced, disseminated, and can be countered». Security and Human Rights 29.1-4 (2018): 55-81
322. Kietzmann, Jan, et al. «Deepfakes: Trick or treat?» Business Horizons 63.2 (2020): 135-146.
323. Kim, Bomi, et al. «The relationship between mother's smartphone addiction and children's smartphone usage». Psychiatry Investigation 18.2 (2021)
324. Kim, Ho-Kyung and Keith E. Davis. «Toward a comprehensive theory of problematic Internet use: Evaluating the role of self-esteem, anxiety, flow, and the self-rated importance of Internet activities». Computers in Human Behavior (2009)
325. Klaassen, Marleen J. E. and Peter Jochen. «Gender (In)equality in Internet Pornography: A Content Analysis of Popular Pornographic Internet Videos» (2014)
326. Kleinman, By Zoe. «My Son Spent £3,160 in One Game». BBC News (2019), www.bbc.com/news/technology-48925623
327. Knorr, Caroline. «Parents' Ultimate Guide to Parental Controls». Common Sense Media (2021), www.commonsensemedia.org/articles/parents-ultimate-guide-to-parental-controls
328. Knutson, Brian, et al. «Dissociation of reward anticipation and outcome with event-related fMRI». Neuroreport 12.17 (2001)
329. Kolodny, Lora. «Securly raises $4 million to put guard rails on the internet for K-12 students». TechCrunch (2016), https://techcrunch.com/2016/10/20/securly-raises-4-million-to-put-guard-rails-on-the-internet-for-k-12-students/
330. Komar, Olha A., et al. «Implementation of a Monitoring System in the Educational Process in Primary School». International Journal of Learning, Teaching and Educational Research Vol. 18 No. 11 (2019)
331. Kondo, Nobuhiko, et al. «Early Detection of At-Risk Students Using Machine Learning Based on LMS Log Data». 6th IIAI International Congress on Advanced Applied Informatics (2017)
332. Konrad, Kerstin, et al. «Brain development during adolescence: neuroscientific insights into this developmental period». Deutsches Ärzteblatt International 110.25 (2013)
333. Kramer, Adam DI, et al. «Experimental evidence of massive-scale emotional contagion through social networks». Proceedings of the National Academy of Sciences 111.24 (2014)
334. Ladd, Gary W. «Peer Rejection, Aggressive or Withdrawn Behavior, and Psychological Maladjustment from Ages 5 to 12: An Examination of Four Predictive Models» (2006)
335. Lafrance, Adrienne. «The Perils of "Sharenting"». The Atlantic 6 (2016).
336. Larsen, Mark Erik, et al. «A systematic assessment of smartphone tools for suicide prevention». PloS one 11.4 (2016)
337. Leibowitz A. «Could Monitoring Students on Social Media Stop the Next School Shooting?» The New York Times (2018), https://www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html
338. Lewak, Doree. «This 6-Year-Old Racked up $16K on Mom's Credit Card Playing Video Games». New York Post (2020), https://nypost.com/2020/12/12/this-6-year-old-racked-up-over-16k-on-his-moms-credit-card/
339. Lin, C., et al. «Internet gaming disorder, psychological distress, and insomnia in adolescent students and their siblings: An actor-partner interdependence model approach» (2021)
340. Livingstone, S., et al. «Children's online activities, risks and safety». UKCCIS (2017)
341. Livingstone, Sonia and Ellen Helsper. «Parental mediation and children's Internet use». Journal of broadcasting and electronic media 52 (4) (2008)
342. Livingstone, Sonia, et al. «Global kids online comparative report» (2019)

343. Lopez, Lori Kido. «The Radical Act of “Mommy Blogging”: Redefining Motherhood through the Blogosphere». New Media & Society, vol. 11, no. 5, (2009): 729–747
344. Lupton, Deborah. «Digital Bodies» (2015)
345. M. Emmison, S. Danby. «Troubles Announcements and Reasons for Calling: Initial Actions in Opening Sequences in Calls to a National Children's Helpline» (2007)
346. M. Hasal, J. Nowaková et al. «Chatbots: Security, privacy, data protection, and social aspects» (2021)
347. Maalla, Najat M’jid. «Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, including the Right to Development» (2009)
348. Mahanta, D. and S. Khatoniyar. «Cyberbullying and Its Impact on Mental Health of Adolescents» (2019)
349. Malachiti, A. «Online Stalking and online activities An evaluation of risks and their perception». (2018)
350. Malo, Sebastien. «Film exposes underworld of U.S. children sold online for sex». Reuters (2017), https://www.reuters.com/article/usa-trafficking-film-idINL1N1FS0L8
351. Mamidipalli, S.S., et al. «Report of Internet Addiction from Indian subcontinent: Diverse in geography but similar in form». Psychol Behav Sci Int J (2017)
352. Marciano, Laura and Anne-Linda Camerini. «Duration, frequency, and time distortion: Which is the best predictor of problematic smartphone use in adolescents? A trace data study». PloS (2022)
353. Martellozzo, E., et al. «I wasn’t sure it was normal to watch it» (2016)
354. Martin, Dominic. «#republic: Divided Democracy in the Age of Social Media». Princeton University Press. Business Ethics Quarterly (2018)
355. Marx, G.T. «What’s in a name? Some reflections on the sociology of anonymity» (1999)
356. Mathur, Arunesh, et al. «Dark patterns at scale: Findings from a crawl of 11K shopping websites». Proceedings of the ACM on Human-Computer Interaction 3.CSCW (2019): 1-32
357. Matteini Palmerini, Riccardo. «Graph theoretical approach to sexual predator detection». NTNU (2021)
358. McCarthy, Christine. «Concerns over TikTok Silhouette Challenge Exposing More than Users Intended». Boston 25 News, (2021), www.boston25news.com/news/local/concerns-over-tiktok-silhouette-challenge-exposing-more-than-users-intended/UPPA6RVIONFDRGTBKZL7N4DOPA
359. McCauley, Denis. «The learning curve: lessons in country performance in education». London: Pearson (2012)
360. McDaniel, Brandon. «Passive sensing of mobile media use in children and families: a brief commentary on the promises and pitfalls». Pediatric Research (2019)
361. McFarlin, L.A., et al. «Usability Impact on Effectiveness of Parental Controls». Proceedings of the Human Factors and Ergonomics Society Annual Meeting (2007)
362. McTigue, Maddy. «Communication Ethics of «Sharenting»: A Content Analysis of Instagram Mom Meso-Influencers» (2021)
363. Mellor, Maria. «Why Is TikTok Creating Filter Bubbles Based on Your Race?» (2020), www.wired.co.uk/article/tiktok-filter-bubbles
364. Melodia, F., et al. «The Role of Avoidance Coping and Escape Motives in Problematic Online Gaming: A Systematic Literature Review» (2020)
365. Meta (ex. Facebook), «Introducing DeepText: Facebook’s text understanding engine» (2016), https://engineering.fb.com/2016/06/01/core-data/introducing-deeptext-facebook-s-text-understanding-engine/
366. Meyer, Marisa, et al. «Advertising in young children's apps: A content analysis». Journal of developmental & behavioral pediatrics 40.1 (2019): 32-39
367. Michaud, Yves. «Les Cahiers Dynamiques». 2014/2 № 60 (2014)
368. Mihara, S. and S. Higuchi. «Cross-sectional and longitudinal epidemiological studies of Internet gaming disorder: A systematic review of the literature» (2015)

369. Mikhailova, Anna. «Theresa May Pledges to Tighten the Law on “Gaslighting” Abuse». The Telegraph (2018), https://www.telegraph.co.uk/politics/2018/05/23/theresa-may-pledges-tighten-law-gaslighting-abuse/
370. Millman, Rene. «20 % of Google Play Apps Breach Child Privacy Rules». IT PRO (2021)
371. Miró-Llinares, Fernando. «That Cyber Routine, That Cyber Victimization: Profiling Victims of Cybercrime» (2015)
372. Mitchell, Amy and Mason Walker. «More Americans Now Say Government Should Take Steps to Restrict False Information Online than in 2018». Pew Research Center (2021)
373. Mitchell, Kimberly, et al. «Trends in Youth Reports of Sexual Solicitations, Harassment and Unwanted Exposure to Pornography on the Internet» (2007)
374. Molloy, Mark. «Wine lovers cannot buy Burgundy tipple on Google as internet giant cracks down on 'gun' searches». The Telegraph, (2018)
375. Moore, H. «A Passion for Difference: Essays in Anthropology and Gender». Cambridge: Polity Press (1994)
376. Morgan, Elizabeth M. «Associations between Young Adults' Use of Sexually Explicit Materials and Their Sexual Preferences, Behaviors, and Satisfaction» (2011)
377. Munro, Eileen. «Predictive analytics in child protection» (2019)
378. Murray, J. «Psychological profile of pedophiles and child molesters» (2000)
379. N. Petrowski, C. Cappa, A. Pereira, H. Mason, R. A. Daban; (2021)
380. National center for Missing & Exploited children «CyberTripline», https://www.missingkids.org/gethelpnow/cybertipline
381. National Human Trafficking Hotline. «Hotline Statistics» (2020)
382. NBC News (2018) «Hackers have taken down dozens of 911 centers. Why is it so hard to stop them?»
383. Nguen, C. «Escape the echo chamber» (2018)
384. Nielsen, J. «UX Design for Children (Ages 3–12)». Nielsen Norman Group
385. Nieminen, Sakari and Lauri Rapeli. «Fighting Misperceptions and Doubting Journalists’ Objectivity: A Review of Fact-checking Literature» (2018)
386. Nussbaum, M. C. «Objectification and internet misogyny» (2010)
387. Nyce, Charles. «Predictive analytics white paper». American Institute for CPCU. Insurance Institute of America (2007)
388. O’Connell, R. «A typology of child cybersexploitation and online grooming practices» (2011)
389. Ongsulee, Parlwat, et al. «Big Data, Predictive Analytics and Machine Learning». 16th International Conference on ICT and Knowledge Engineering (2018)
390. Ophir, Yaakov, et al. «Deep neural networks detect suicide risk from textual facebook posts». Scientific Reports (2020)
391. Optional protocol to the Convention on the Rights of the child on the sale of children, child prostitution and child pornography
392. Orcutt, Ashley Mae. «State of Internet Scams» (2021), https://socialcatfish.com/blog/state-of-internet-scams-2021/
393. Ouvrein, Gaëlle and Karen Verswijvel. «Sharenting: Parental adoration or public humiliation? A focus group study on adolescents' experiences with sharenting against the background of their own impression management». Children and Youth Services Review 99 (2019): 319-327.
394. Pangrazio, Luci. «Apps That Help Parents Protect Kids from Cybercrime May Be Unsafe Too». The Conversation (2021)
395. Papadamou, Kostantinos, et al. «Disturbed YouTube for kids: Characterizing and detecting inappropriate videos targeting young children». Proceedings of the international AAAI conference on web and social media. Vol. 14. (2020)
396. Pariser, Eli. «The filter bubble: How the new personalized web is changing what we read and how we think». Penguin (2011)
397. Paulus, F., et al. «Internet gaming disorder in children and adolescents: a systematic review» (2018)

398. Perez, Sarah. «YouTube to launch parental control features for families with tweens and teens». TechCrunch (2021), https://techcrunch.com/2021/02/24/youtube-to-launch-parental-control-features-for-families-with-tweens-and-teens/
399. Perrotta, G. «Pedophilia: Definition, classifications, criminological and neurobiological profiles, and clinical treatments. A complete review» (2020)
400. Perrotta, G. «Psicologia dinamica» (2019)
401. Pescaro, Mike. «TikTok Outlet Challenge: 2 Students Being Charged After 8 Outlets Damaged at Mass. School». NBC10 Boston (2020), https://www.nbcboston.com/news/local/tiktok-outlet-challenge-2-students-being-charged-after-8-outlets-damaged-at-mass-school/2068830/
402. Pina, A., et al. «An overview of the literature on sexual harassment: Perpetrator, theory, and treatment issues» (2009)
403. Przybylski, A. K. and V. Nash. «Internet Filtering Technology and Aversive Online Experiences in Adolescents» (2017)
404. Przybylski, A. K. et Victoria Nash. «Internet filtering and adolescent exposure to online sexual material». Cyberpsychology, behavior and social networking Vol. 21 No. 7 (2018)
405. Przybylski, A. K., et al. «Internet Gaming Disorder: Investigating the Clinical Relevance of a New Phenomenon». (2016)
406. Purcell, R., et al. «Stalking among juveniles» (2009)
407. Q. Xu, M. Zhang. «The Research on Critical Factors Affecting the Game Experience of Daily Quests System in Mobile Game». (2020)
408. Quadara, Antonia, et al. «The effects of pornography on children and young people» (2017)
409. Ra, Chaelin K., et al. «Association of digital media use with subsequent symptoms of attention-deficit/hyperactivity disorder among adolescents». Jama (2018), https://jamanetwork.com/journals/jama/article-abstract/2687861
410. Rahman, Zara and Julia Keseru. «Predictive Analytics for Children: An assessment of ethical considerations, risks, and benefits». UNICEF Innocenti Research (2021)
411. Reece, Andrew G. and Christopher M. Danforth. «Instagram photos reveal predictive markers of depression». EPJ Data Science 6.1 (2017)
412. Reyns, Bradford and Bonnie Fisher. «The Relationship Between Offline and Online Stalking Victimization: A Gender-Specific Analysis» (2018)
413. Rieger, Sebastian and Caroline Sinders. «Dark Patterns: Regulating Digital Design». SNV (2020)
414. Rinehart, Aimee. «Fake News. It's Complicated» (2021)
415. Rose, M. «The average parent shares almost 1,500 images of their child online before their 5th birthday». Parentzone (2018), https://parentzone.org.uk/article/average-parent-shares-almost-1500-images-their-child-online-their-5th-birthday
416. Rosenbloom, Maxie. «Request for Public Comment on the Federal Trade Commission's Request for Comments Regarding Topics to be Discussed at Dark Patterns Workshop» (2021)
417. Rosenbloom, Michael. «Dark patterns». (2021)
418. Rosie Shrout, M. and Daniel J. Weigel. «Infidelity's aftermath: Appraisals, mental health, and health-compromising behaviors following a partner's infidelity» (2017)
419. Rothman, E.F., et al. «The Prevalence of Using Pornography for Information About How to Have Sex: Findings from a Nationally Representative Survey of U.S. Adolescents and Young Adults» (2021)
420. Salin, D., et al. «Workplace bullying across the globe: a cross-cultural comparison» (2018)
421. Santos, Fernando P., et al. «Link recommendation algorithms and dynamics of polarization in online social networks». Proceedings of the National Academy of Sciences 118.50 (2021)
422. Scharenbroch, Chris, et al. «Principles for Predictive Analytics in Child Welfare». Children Research Center (2017)

423. Schmuck, Desirée. «Following Social Media Influencers in Early Adolescence: Fear of Missing Out, Social Well-Being and Supportive Communication with Parents». Journal of Computer-Mediated Communication 26.5 (2021): 245-264
424. Schüll, Natasha Dow. «Addiction by design». Princeton University Press (2012)
425. Sciences and Technologies for Security Applications (2018)
426. Security Industry Association. « Face Facts: Dispelling Common MYTHS. Associated With Facial Recognition Technology»
427. Sequeira, Lydia, et al. «Mobile and wearable technology for monitoring depressive symptoms in children and adolescents: A scoping review». Journal of Affective Disorders, Volume 265 (2020)
428. Shah, Sabir. «Interesting Statistics about Fake News on Social Media». The News International (2021),
https://www.thenews.com.pk/print/893091-interesting-statistics-about-fake-news-on-social-media
429. Sharma, Manoj Kumar and Poornima Mahindru. «Video game addiction: Impact on teenagers' lifestyle». Natl Med J India (2015)
430. Shek, Daniel T. L., et al. «The influence of parental control and parent-child relational qualities on adolescent internet addiction: a 3-year longitudinal study in Hong Kong». Frontiers in psychology (2018)
431. Sheridan, Lorraine, et al. «Stalking and age» (2014)
432. Simon, L. «An Examination of the Assumptions of Specialization, Mental Disorder, and Dangerousness in Sex Offenders». Behavioral Sciences and the Law (2000)
433. Sivak, Elizaveta and Ivan Smirnov. «Parents mention sons more often than daughters on social media». Proceedings of the National Academy of Sciences 116.6 (2019): 2039-2041
434. Slavich, George, et al. «Stress measurement using speech: Recent advancements, validation issues, and ethical and privacy considerations» (2019)
435. Smahel, David, et al. «EU Kids Online 2020. Survey results from 19 countries»
436. Snyder, P., et al. «Internet Measurement Conference». (2017)
437. Song, Felicia Wu. «The Serious Business of Mommy Bloggers». Contexts, vol. 15, no. 3 (2016): 42–49
438. Song, Juyoung, et al. «Social Big Data Analysis of Future Signals for Bullying in South Korea: Application of General Strain Theory». Telematics and Informatics (2020)
439. Sourander, A., et al. «Psychosocial Risk Factors Associated With Cyberbullying Among Adolescents» (2010)
440. Spalevic, Zaklina and Milos Ilic. «The use of dark web for the purpose of illegal activity spreading». Ekonomika, Journal for Economic Theory and Practice and Social Issues (2017)
441. Spathis, Dimitris, et al. «Passive mobile sensing and psychological traits for large scale mood prediction» (2019)
442. Stachl, Clemens, et al. «Predicting personality from patterns of behavior collected with smartphones». Proceedings of the National Academy of Sciences 117.30 (2020)
443. Stahl, S. and I. Dennhag. «Online and offline sexual harassment associations of anxiety and depression in an adolescent sample» (2020)
444. Staksrud, Elisabeth, et al. «What Do We Know About Children’s Use of Online Technologies? A Report on Data Availability and Research Gaps in Europe» (2007)
445. Stanley, Janet Robin. «Child Abuse and the Internet» (2001)
446. Starbird, Kate, et al. «Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations». Proceedings of the ACM on Human-Computer Interaction 3.CSCW (2019): 1-26
447. Stark, Phillip B. «The effectiveness of internet content filters». University of California (2007)
448. Stevens, MW, et al. «Global prevalence of gaming disorder: A systematic review and meta-analysis». (2021)
449. Stoilova, Mariya and Sonia Livingstone. «The 4Cs: Classifying online risk to children» (2021)
450. Stoner, James A. F. «Risky and cautious shifts in group decisions: The influence of widely held values». Journal of Experimental Social Psychology (1968)

451. Suciu, Peter. «Spotting Misinformation On Social Media Is Increasingly Challenging». Forbes (2021), https://www.forbes.com/sites/petersuciu/2021/08/02/spotting-misinformation-on-social-media-is-increasingly-challenging/
452. Suk, William A. et al. «Environmental hazards to children's health in the modern world». Mutation Research/Reviews in Mutation Research (2003): 235-242
453. Sunde, Nina and Inger Marie Sunde. «Conceptualizing an AI-based Police Robot for Preventing Online Child Sexual Exploitation and Abuse». Nordic Journal of Studies in Policing (2021)
454. Sundquist, Joanna Sanchez. «The problem of child pornography». UMEA University (2020)
455. Suwastini, Ni Komang Arie, et al. «The dangerous trend among teenagers analyzed: social media as academic research». The fourth International Conference on English across cultures (2018)
456. Sweet, Paige L. «The sociology of gaslighting». American Sociological Review 84.5 (2019): 851-875.
457. T.Bell. «How Software Is Taking On School Shootings». Fast Company, 14 Feb. (2018)
458. Tanner, Lindsey. «Detecting depression: Smartphone apps could monitor teen angst». The Denver Post (2019), www.denverpost.com/2019/01/14/apps-detect-teenage-depression-angst/
459. Tartari, Elda. «Benefits and risks of children and adolescents using social media». European Scientific Journal vol. 11 No. 13 (2015)
460. Taylor, Max and Ethel Quayle. «Child Pornography: An Internet Crime». (2003)
461. Teng, Z., et al. «Depression and anxiety symptoms associated with internet gaming disorder before and during the COVID-19 pandemic: A longitudinal study». (2021)
462. Thacker, R. and S. Gohmann. «Emotional and Psychological Consequences of Sexual Harassment: A Descriptive Study» (1996)
463. The Office of the Privacy Commissioner for Personal Data
464. Tolosana, Ruben, et al. «Deepfakes and beyond: A survey of face manipulation and fake detection». Information Fusion 64 (2020): 131-148.
465. Torous, John, et al. «Smartphones, Sensors, and Machine Learning to Advance Real-Time Prediction and Interventions for Suicide Prevention: a Review of Current Progress and Next Steps». Curr Psychiatry Rep 20, 51 (2018)
466. Turel, Ofir, et al. «Health outcomes of information system use lifestyles among adolescents: videogame addiction, sleep curtailment and cardio-metabolic deficiencies». PloS one 11.5 (2016)
467. Vaccari, Cristian and Andrew Chadwick. «Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news». Social Media+ Society 6.1 (2020)
468. Van Deursen, Alexander JAM, et al. «Modeling habitual and addictive smartphone behavior: The role of smartphone usage types, emotional intelligence, social stress, self-regulation, age, and gender». Computers in human behavior 45 (2015): 411-420.
469. Vannier, Sarah A., et al. «Schoolgirls and Soccer Moms: A Content Analysis of Free «Teen» and «MILF» Online Pornography». (2014)
470. Vidua, R., et al. «Suicide linked to PUBG video gaming: A case report». (2020)
471. Vosoughi, Soroush, et al. «The spread of true and false news online». Science 359.6380 (2018): 1146-1151
472. Vziatysheva, Victoria. «How fake news spreads online?» International Journal of Media and Information Literacy 5 (2020): 217-226.
473. Wakefield, By Jane. «TikTok Skull-Breaker Challenge Danger Warning». BBC News (2020), www.bbc.com/news/technology-51742854
474. Walter, Nathan, et al. «Fact-checking: A meta-analysis of what works and for whom». Political Communication 37.3 (2020): 350-375
475. Warentest, Stiftung. «Unsichere Kinderprodukte». (2018)
476. Watson, Amy. «Fake News in the U.S. — Statistics and Facts». Statista (2021), https://www.statista.com/topics/3251/fake-news/
477. Webster, Stephen, et al. «European Online Grooming: Project final report» (2012)

478. Weller, Orion, et al. «Predicting suicidal thoughts and behavior among adolescents using the risk and protective factor framework: A large-scale machine learning approach» (2021)
479. Westerlund, Mika. «The emergence of deepfake technology: A review». Technology Innovation Management Review 9.11 (2019)
480. Whang, Leo Sang-Min, et al. «Internet Over-Users' Psychological Profiles: A Behavior Sampling Analysis on Internet Addiction». CyberPsychology & Behavior (2003)
481. Whitcomb, Dan. «Florida man imprisoned for trafficking girl, 14, via Backpage.com». Reuters (2019), https://www.reuters.com/article/us-florida-humantrafficking-idUSKCN1S62IK
482. Whyte, Jennifer. «The future of systems integration within civil infrastructure: A review and directions for research. INCOSE International Symposium» (2016)
483. Williamson, Ben. «Digital education governance: data visualization, predictive analytics, and “real-time” policy instruments». Journal of education policy 31.2 (2016)
484. Wilson, Michael. «Pizza Orders Reveal Credit Card Scheme, and a Secondhand Market». New York Times (2014), https://www.nytimes.com/2014/12/06/nyregion/pizza-orders-reveal-credit-card-scheme-and-a-secondhand-market.html
485. Winkler, Matt, et al. «Toy safety surveillance from online reviews». Decision support systems 90 (2016): 23-32
486. Wisniewski, Pamela, et al. «Parental control vs. teen self-regulation: is there a middle ground for mobile online safety?» ACM Conference on computer supported cooperative work and social computing (2017)
487. Wittek, C., et al. «Prevalence and Predictors of Video Game Addiction: A Study Based on a National Representative Sample of Gamers» (2016)
488. Wolak, Janis, et al. «1 in 7 Youth: The Statistics about Online Sexual Solicitations» (2007)
489. Wolfowicz, M. et al. «Examining the interactive effects of the filter bubble and the echo chamber on radicalization» (2021)
490. Wood, Jessica A. «The Darknet: A Digital Copyright Revolution». Richmond Journal of Law & Technology 16.4 (2009)
491. Wortley, Richard and Stephen Smallbone. «Child pornography on the Internet» Problem-Specific Guides Series. Problem-Oriented Guides for Police № 41 (2012)
492. Heilweil, Rebecca. «Algorithms and Bias, Explained». Vox (2020), www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency
493. Xiuqin, Huang, et al. «Mental health, personality, and parental rearing styles of adolescents with Internet addiction disorder». Cyberpsychology, Behavior and Social Networking 13 (2010)
494. Xu, J. «A deep learning approach to building an intelligent video surveillance system. Multimed Tools» Appl 80, 5495–5515 (2021)
495. Ye, Liang et al. «A Video-Based DT-SVM School Violence Detecting Algorithm». Sensors (Basel, Switzerland) vol. 20,7 (2020)
496. Yuvaraj, T. and Dr. Suresh A. «A review on the definitions of internet overuse behavior». (2018)
497. Zamani, E., et al. «Effect of Addiction to Computer Games on Physical and Mental Health of Female and Male Students of Guidance School in City of Isfahan» (2009)
498. Zendle, David, et al. «The prevalence of loot boxes in mobile and desktop games». Addiction 115.9 (2020): 1768-1772
499. Zhitomirsky-Geffet, Maayan and Maya Blau. «Cross-generational analysis of predictive factors of addictive behavior in smartphone usage». Comput. Hum. Behav. 64 (2016)
500. Zilka, Gila Cohen. «Awareness of eSafety and potential online dangers among children and teenagers». Journal of Information Technology Education: Research 16 (2017)
501. Zilli, Arturo. «Could Social Network Analysis Be a Useful Tool to Disarticulate Criminal Networks?» Academia (2021)

502. Zinzow, H., et al. «Prevalence and risk of psychiatric disorders as a function of variant rape histories: results from a national survey of women» (2012)
503. Zuiderveen Borgesius, Frederik, et al. «Should we worry about filter bubbles?» Internet Policy Review. Journal on Internet Regulation 5.1 (2016)
504. «10 Fake Grassroots Movements Started By Corporations To Sway Your Opinion». Insider (2011), https://www.businessinsider.com/astroturfing-grassroots-movements-2011-9
505. «2 plead guilty in one of largest child pornography cases in US history». U.S. Immigration and Customs Enforcement (2013), https://www.ice.gov/news/releases/2-plead-guilty-one-largest-child-pornography-cases-us-history
506. «37th Semi-Annual Taking Stock With Teens Survey». Piper Sandler (2021)
507. «A parent's guide to Internet Filtering and Monitoring». Axis (2018)
508. «A parents' guide to filtering technologies. Get with it!» Brunswick Press Ltd. (2010)
509. «Algorithmic Bias: Why And How Do Computers Make Unfair Decisions?» LibertiesEU (2021), www.liberties.eu/en/stories/algorithmic-bias-17052021/43528
510. «American Academy of Pediatrics: children, adolescents and television». Pediatrics 107.2 (2001): 423-426
511. «Animal Jam was hacked, and data stolen; here's what parents need to know». TechCrunch (2020), https://techcrunch.com/2020/11/16/animal-jam-data-breach/
512. «Ashley Madison condemns attack as experts say hacked database is real». The Guardian (2015), https://www.theguardian.com/technology/2015/aug/19/ashley-madisons-hacked-customer-files-posted-online-as-threatened-say-reports
513. «Ashley Madison hacked, users threatened with exposure». CBS News (2015), https://www.cbsnews.com/news/ashley-madison-hacked-users-threatened-with-exposure/
514. «Ashley Madison parent in $11.2 million settlement over data breach». Reuters (2015), https://www.reuters.com/article/us-ashleymadison-settlement-idUSKBN19Z2F0
515. «Ashley Madison users now facing extortion». CNN Business (2015), https://money.cnn.com/2015/08/21/technology/ashley-madison-users-extorted/
516. «Ashley Madison: Suicides over website hack». BBC (2015), https://www.bbc.com/news/technology-34044506
517. «BBFC Research into Children and Pornography». BBFC (2019)
518. «Big tobacco bankrolls anti-Labor ad campaign». ABC News (2010), https://www.abc.net.au/news/2010-08-04/big-tobacco-bankrolls-anti-labor-ad-campaign/931280
519. «Billie Eilish says watching porn as a child "destroyed my brain"». The Guardian (2021), https://www.theguardian.com/music/2021/dec/15/billie-eilish-says-watching-porn-gave-her-nightmares-and-destroyed-my-brain
520. «Body Image in Childhood». Mental Health Foundation (2020)
521. «Body of Missing Student at Brown Is Discovered». New York Times (2013), https://edition.cnn.com/2013/04/25/us/rhode-island-missing-brown-student/index.html
522. «Boston bombing: How internet detectives got it very wrong». BBC (2013), https://www.bbc.com/news/technology-22214511
523. «Campaign for a Commercial-Free Childhood». Center for Digital Democracy (2021)
524. «Chamath Palihapitiya, Founder and CEO Social Capital, on Money as an Instrument of Change». Stanford Graduate School of Business (2017)
525. «Chapter v traffickers use of the Internet». UNODC (2020)
526. «Child Identity Fraud Study». Javelin Strategy (2018), https://www.javelinstrategy.com/coverage-area/2018-child-identity-fraud-study
527. «Child Identity Fraud: A Web of Deception and Loss». Javelin Strategy (2021), https://www.javelinstrategy.com/coverage-area/child-identity-theft-fraud
528. «Child Privacy in the Age of Web 2.0 and 3.0: Challenges and opportunities for policy». UNICEF (2017), https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf

529. «Child Safety Online: Global challenges and strategies». UNICEF. Technical Report (2012)
530. «Children and parents: media use and attitudes report». Ofcom (2021)
531. «Children's Online Privacy Protection Rule». Federal Trade Commission (2013)
532. «Connecticut Boy, 6, Racked up $16K Bill on His Mom's Credit Card Playing Video Games on Her IPad». Daily Mail (2020), https://www.dailymail.co.uk/news/article-9048605/Connecticut-boy-6-racked-16K-bill-moms-credit-card-playing-video-games-iPad.html
533. «Cyberbullying: A global advisor survey». Ipsos Public Affairs (2018)
534. «Cyberbullying». Pew Research Center (2007)
535. «Diagnostic and Statistical Manual of Mental Disorders. 5th edn». American Psychiatric Association (2013)
536. «Digital advertising spending worldwide from 2019 to 2024». Statista (2021)
537. «Digital Wellbeing 2020». The Cybersmile Foundation (2021)
538. «Don't judge Ashley Madison users too quickly, their accounts may be fake». Per Tornstein (2015)
539. «E-commerce: conversion thanks to real-time age verification». Deutsche Bank AG (2018), https://developer.db.com/products/dbAPI_CaseStudy_madco_EN.pdf
540. «Eleventh report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat» (2020)
541. «Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You». Time (2018)
542. «Fake news worldwide — statistics & facts». Statista (2021), https://www.statista.com/topics/6341/fake-news-worldwide/#dossierKeyfigures
543. «Filter Bubble – A Built-In Bias in Your Social Media Feed and Searches». Aarambh Child Protection (2021), http://aarambhindia.org/filter-bubble-built-bias-social-media-feed-searches/
544. «Filter bubbles are a serious problem with news, says Bill Gates». Quartz (2017)
545. «First World Report on Violence and Health». World Health Organization (2002)
546. «Gainesville Man Sentenced to 120 Months in Prison for Obtaining Minor for Commercial Sex». Department of Justice U.S. Attorney's Office, Northern District of Florida (2019)
547. «Girl starved to death while parents raised virtual child in online game». The Guardian (2010), https://www.theguardian.com/world/2010/mar/05/korean-girl-starved-online-game
548. «Global Report on Trafficking in Persons». UNODC (2018)
549. «Good Use and Abuse: The Role of Technology in Human Trafficking». United Nations Office on Drugs and Crime (2021)
550. «Hackers expose first Ashley Madison users». CBS News (2015), https://www.cbsnews.com/news/hackers-expose-first-ashley-madison-users/
551. «Hackers Finally Post Stolen Ashley Madison Data». WIRED (2015), https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/
552. «Half of Children and Teens Exposed to Harmful Online Content While in Lockdown». BBFC (2020), https://www.bbfc.co.uk/about-us/news/half-of-children-and-teens-exposed-to-harmful-online-content-while-in-lockdown
553. «Handbook on Children Recruited and Exploited by Terrorist and Violent Extremist Groups: The Role of the Justice System». UN (2017)
554. «Harm being done to Australian children through access to pornography on the Internet». Church and nation committee
555. «Harvard Rescinds Acceptances for At Least Ten Students for Obscene Memes | News | The Harvard Crimson». The Harvard Crimson (2017), www.thecrimson.com/article/2017/6/5/2021-offers-rescinded-memes
556. «High Amounts of Screen Time Begin as Early as Infancy, NIH Study Suggests». National Institutes of Health (2019),

www.nih.gov/news-events/news-releases/high-amounts-screen-time-begin-early-infancy-nih-study-suggests
557. «How Media Use Can Affect Kids (for Parents) — Nemours KidsHealth». KidsHealth (2021), kidshealth.org/en/parents/tv-affects-child.html
558. «How Reddit Fueled the Scanner-Happy Media to Out Innocent Boston 'Suspects'». The Atlantic (2013), https://www.theatlantic.com/technology/archive/2013/04/reddit-police-scanner-innocent-boston-suspects/316101/
559. «How to prevent online harassment from doxxing». U.S. Department of Homeland Security
560. «How to prevent your kids from bypass parental controls». TechTricksZone (2021), https://techtrickszone.com/prevent-your-kids-from-bypass-parental-controls/
561. «Impact of media use on children and youth». Paediatr Child Health (2003)
562. «Instagram, Facebook, and the Perils of “Sharenting”» The New Yorker (2019), www.newyorker.com/culture/cultural-comment/instagram-facebook-and-the-perils-of-sharenting
563. «Interesting statistics about fake news on social media». The International News (2021)
564. «International Classification of Diseases-11». WHO (2018)
565. «Internet fraud — seniors and teenagers». Citywide banks, https://www.citywidebanks.com/sites/heartland/files/1232_18_Internet_Fraud_Retail.pdf
566. «Internet monitoring software to control cyber-bulling In schools». PearlSoftware, www.pearlsoftware.com/solutions/cyberbullying-in-schools.html
567. «Internet Overuse and Addiction». The University of Melbourne, services.unimelb.edu.au/counsel/resources/addictive-behaviours/internet-overuse-and-addiction
568. «Kayleigh Haywood: How murdered schoolgirl was groomed online». BBC News (2016), https://www.bbc.com/news/uk-england-leicestershire-36606210
569. «Kids for Sale: Online Advertising and the manipulation of children». Global Action Plan (2020)
570. «Kids interact at home with predators – via social media». The Times (2017), https://www.shreveporttimes.com/story/news/investigations/2017/05/25/kids-interact-predators-home-via-social-media/101801508/
571. «Life in likes: Children’s Commissioner Report into social media use among 8–12 year olds». Children’s Commissioner (2018)
572. «Man Sentenced to 30 Years for Production of Child Pornography». The United States Department of Justice (2022), https://www.justice.gov/opa/pr/man-sentenced-30-years-production-child-pornography
573. «Massachusetts Students Face Criminal Charges after Viral “Outlet Challenge” Damages School». New Bedford Guide (2020), www.newbedfordguide.com/massachusetts-viral-outlet-challenge/2020/01/29.
574. «Microsoft research on cyberbullying in various countries worldwide». Microsoft (2012)
575. «Most common forms of cyber stalking an ex or current partner online according to adults in the United States as of December 2019». Statista (2021), https://www.statista.com/statistics/1189386/cyber-stalking-ex-current-partner-online/
576. «Most common negative online experiences according to global internet users as of June 2016». Statista (2016), https://www.statista.com/statistics/675947/negative-online-experiences/
577. «My Teenage Daughter’s Social Media Use Has Become Really Obsessive». The Irish Times (2019)
578. «Neo-Nazi Matthew Cronjager jailed for plotting terrorist acts». BBC (2021), https://www.bbc.com/news/uk-england-essex-58973060
579. «New Kids Helpline Data Reveals Spike in Duty of Care Interventions». Yourtown, 9 June 2021, www.yourtown.com.au/media-centre/new-kids-helpline-data-reveals-spike-duty-care-interventions.
580. «News Conference Re: Ashley Madison Website Hack». Police of Toronto (2015)

581. «Number of reports of stalking in Italy in 2019, by gender of perpetrator». Statista (2021), https://www.statista.com/statistics/1077812/distribution-of-reports-of-stalking-by-gender-in-italy/
582. «Online security apps focus on parental control, not teen self-regulation». Science Daily (2017)
583. «Online violence has real life consequences #ItIsMyBusiness». UNDP Serbia (2021), https://www.rs.undp.org/content/serbia/en/home/presscenter/articles/2021/digitalno-nasilje-ostavlja-stvarne-posledice.html
584. «Overblocking and underblocking in network level filters». Parliament UK, https://publications.parliament.uk/pa/cm201617/cmpublic/digitaleconomy/memo/DEB63.pdf
585. «Parental Controls», Childnet, www.childnet.com/help-and-advice/parental-controls/
586. «Pathways: How digital design puts children at risk», 5Rights Foundation (2021), https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf
587. «Percentage of U.S. middle and high school students who were cyber bullied as of April 2019, by type of bullying and gender». Statista (2021), https://www.statista.com/statistics/291034/cyber-bullying-share-of-us-students-by-type-and-gender/
588. «Perfomance report». AEPD (2021), www.aepd.es/sites/default/files/2020-04/nota-tecnica-protection-of-minors-on-the-internet-en.pdf
589. «Personal data misuse experienced by children in the CEE region 2017-2019». Statista, https://www.statista.com/statistics/1190588/cee-personal-data-misuse-experienced-by-children-by-age/
590. «Preventing Terrorism and Countering Violent Extremism and Radicalization That Lead to Terrorism: A Community-Policing». OSCE (2014)
591. «Protecting children from harmful marketing practices». WHO-UNICEF-Lancet Commission (2020)
592. «Protection of Minors in the Audiovisual Media Services: Trends & Practices». ERGA, https://erga-online.eu/wp-content/uploads/2016/10/ERGA-PoM-Report-2017-wordpress.pdf
593. «Raising the smartphone generation. New research into how parents and children manage their digital habits». Kaspersky, www.kaspersky.com/blog/digital-habits-report-2021/
594. «Retail group quits cigarette label campaign». ABC News (2010), https://www.abc.net.au/news/2010-08-11/retail-group-quits-cigarette-label-campaign/939914
595. «Roommate in Tyler Clementi Case Pleads Guilty to Attempted Invasion of Privacy». New York Times (2016), https://www.nytimes.com/2016/10/28/nyregion/dharun-ravi-tyler-clementi-case-guilty-plea.html
596. «Safety alert: Serious button battery and magnet dangers in online marketplace toys». Which (2021), https://www.which.co.uk/news/2021/08/safety-alert-serious-button-battery-and-magnet-dangers-in-online-marketplace-toys/
597. «Safety in Educational Toys». Edx Education (2021), https://edxeducation.com/safety-in-educational-toys/
598. «Set Up Parental Controls on Your Fire Tablet». Amazon, www.amazon.com/gp/help/customer/display.html?nodeId=GG2LBLF5V2T8XUX8
599. «Situation Report Trafficking in human beings in the EU». Europol (2014)
600. «Social Media: help and advice». Childnet.com, https://www.childnet.com/help-and-advice/social-media/
601. «Social networks for kids and why they failed». Kaspersky (2016), https://kids.kaspersky.com/social-networks-for-kids/
602. «Stalker 'found Japanese singer through reflection in her eyes». BBC (2019), https://www.bbc.com/news/world-asia-50000234
603. «Stalking Facts». Stalking Prevention, Awareness & Resource Center
604. «Student Reports of Bullying: Results From the 2017 School Crime Supplement to the National Crime Victimization Survey». U.S. DEPARTMENT OF EDUCATION (2019)

605. «Survey on the Gaming Habits among Hong Kong Upper Primary Students: major findings and conclusion». The University of Hong Kong (2017)
606. «Teaching Kids to Be Smart About Social Media». KidsHealth.org (2020)
607. «Teaching presence». Pearson Education (2016)
608. «Teens and the Screen study: Exploring Online Privacy, Social Networking and Cyberbullying». McAfee (2014)
609. «Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse». Interagency working group on sexual exploitation of children (2016)
610. «The best social networks for younger children». Welivesecurity.com (2020), https://www.welivesecurity.com/2020/06/01/best-social-networks-younger-children/
611. «The Facebook Whistleblower Says Its Algorithms Are Dangerous. Here's Why». MIT Technology Review (2021)
612. «The kids emptied our bank account playing Fifa». BBC (2019), https://www.bbc.com/news/technology-48908766
613. «The man who posed as his daughter's online boyfriend to get nude photos of her». The Washington Post (2016), https://www.washingtonpost.com/news/true-crime/wp/2016/03/17/the-man-who-posed-as-his-daughters-online-boyfriend-to-get-nude-photos-of-her/
614. «The State of Stalkerware in 2020». Kaspersky (2020)
615. «The Teenager Pictured On New York Post Front Page Goes To Police To Clear Name». Business Insider (2013)
616. «Toy Recall Statistics». United States Consumer Product Safety Commission (2015), http://www.cpsc.gov/en/Safety-Education/Toy-Recall-Statistics/
617. «Toy-Related Deaths and Injury Calendar». United States Consumer Product Safety Commission (2015), http://www.cpsc.gov/Global/
618. «Traffickers abusing online technology, UN crime prevention agency warns». United Nations (2021)
619. «UK online pornography age block triggers privacy fears». The Guardian (2019), https://www.theguardian.com/culture/2019/mar/16/uk-online-porn-age-verification-launch
620. «Views on student activity monitoring software». Center for democracy and technology (2021), https://cdt.org/wp-content/uploads/2021/09/Student-Activity-Monitoring-Software-Polling-Research-Slides.pdf
621. «Violence against children during COVID-19: Assessing and understanding change in use of helplines, Child Abuse & Neglect»
622. «Violence in the media: Psychologists study potential harmful effects». American Psychological Association (2013), https://www.apa.org/topics/video-games/violence-harmful-effects
623. «Voters Don't Trust Media Fact-Checking». Rasmussen Reports (2016)
624. «Welsh gamer jailed for grooming two boys on Minecraft». The Guardian (2017), https://www.theguardian.com/uk-news/2017/jan/20/welsh-gamer-jailed-for-grooming-two-boys-on-minecraft
625. «What Bark monitors». Официальный сайт сервиса родительского контроля Bark Technologies, https://bark.us/what-bark-monitors
626. «What is cyberbullying and how to stop it». UNICEF
627. «What is disinformation». Bundesregierung. Startseite, German Federal Government (2021)
628. «What Is Freemium?» Investopedia (2021), www.investopedia.com/terms/f/freemium.asp
629. «What is Stalking?» Stalking Prevention, Awareness, & Resource Center
630. «Why advertising is bad for children». Projeto Criança e Consumo (2009)
631. «Why financial scams may be the biggest cyber-threat to your children». Newscentre.Vodafone (2021), https://newscentre.vodafone.co.uk/smart-living/digital-parenting/why-financial-scams-may-be-the-biggest-cyber-threat-to-your-children/

632. «Why Generation Z Falls for Online Misinformation». MIT Technology Review (2021)
633. «Why kids love TikTok Challenges». Psychology Today (2021), https://www.psychologytoday.com/us/blog/positively-media/202102/why-kids-love-tiktok-challenges
634. «Xanax, Ecstasy, and Opioids: Instagram Offers Drug Pipeline to Kids». Tech Transparency Project (2021)
635. «Young people, pornography & age-verification». BBFC (2020)
636. «Young people's experiences of online sexual harassment». Project «dsSHAME» report (2017)

На момент публикации этого отчета ряд источников могли быть признаны выполняющими роль иностранного агента.