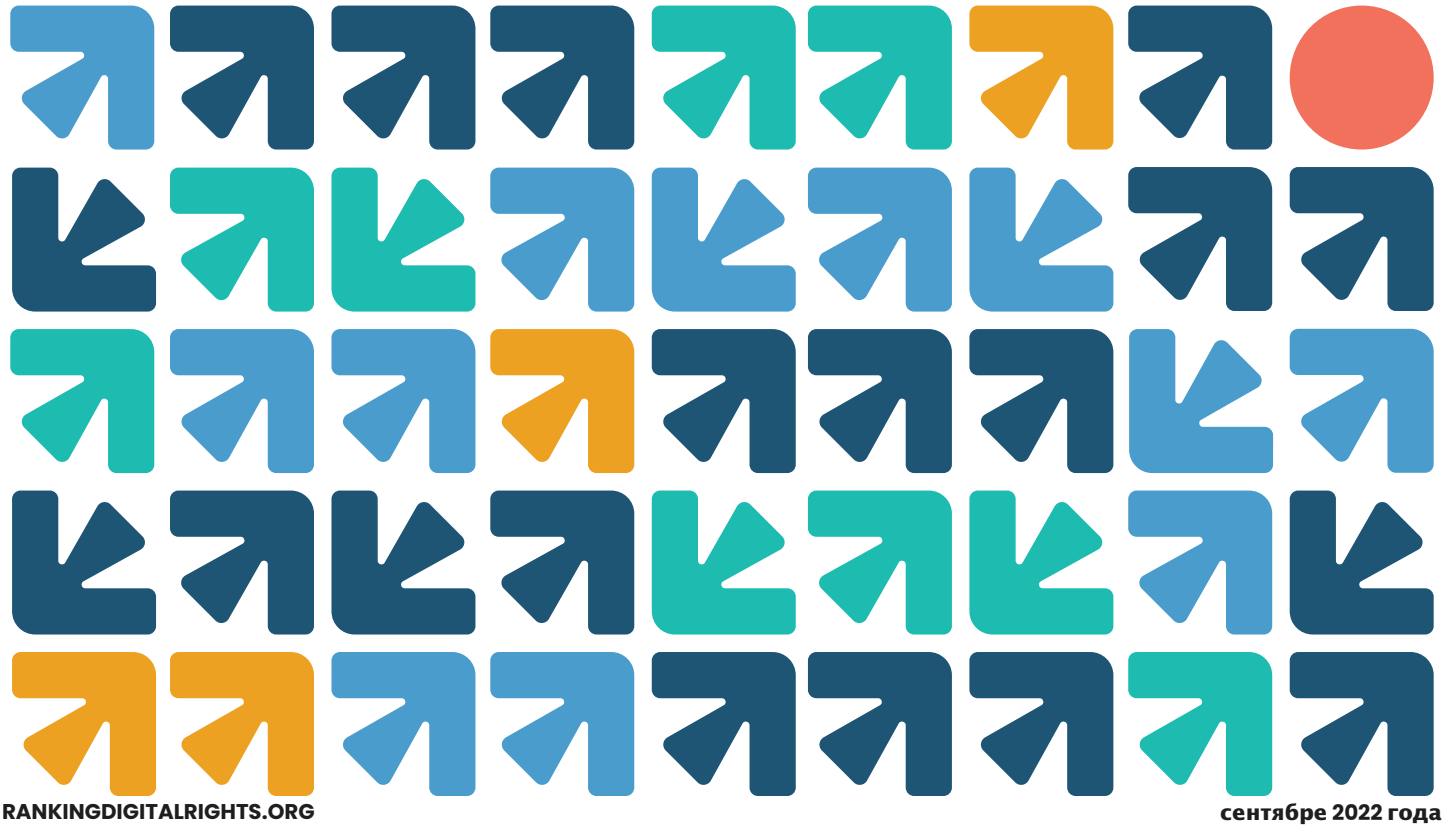
Ranking Digital Rights

# Индекс ответственности корпораций за 2020 год: индикаторы для исследования

## Содержит руководство по индикаторам и глоссарий



## Благодарности

В разработке методологии Индекса ответственности корпораций за 2020 год и установлении контактов с заинтересованными сторонами принимали участие следующие члены команды Рейтинга цифровых прав (Ranking Digital Rights, RDR):

- Эми Брулетт (Amy Brouillette), директор по исследованиям
- Весна Вессенауэр (Veszna Wessenauer), руководитель исследования
- Натали Маршаль (Nathalie Maréchal), старший аналитик в области политик
- Афеф Абруги (Afef Abrougui), аналитик-исследователь
- Зак Рогофф (Zak Rogoff), аналитик-исследователь
- Ян Рыдзак (Jan Rydzak), ведущий специалист по вовлечению компаний и аналитик-исследователь
- Цзе Чжанг (Jie Zhang), аналитик-исследователь

Все участники проекта представлены здесь:
https://rankingdigitalrights.org/who/ [анг]

Команда RDR выражает благодарность каждому из более ста представителей заинтересованных сторон, которые давали отзывы и вносили предложения на протяжении всего процесса разработки этой методологии. Также мы хотим отметить вклад бывших членов команды RDR Лоры Рид (Laura Reed) и Андреа Хакль (Andrea Hackl) за неоценимый вклад на раннем этапе работы над этим проектом в начале 2019 года.

## О Рейтинге цифровых прав (RDR)

Рейтинг цифровых прав (Ranking Digital Rights, RDR) — некоммерческая исследовательская инициатива, созданная под эгидой Института открытых технологий (Open Technology Institute) при проекте New America. Совместно с сетью международных партнеров RDR работает над составлением свода общих стандартов для компаний из сектора информационно-коммуникационных технологий (ИКТ) в вопросах соблюдения прав человека на самовыражение и приватность.

Дополнительную информацию о Рейтинге цифровых прав (RDR) и его Индексе ответственности корпораций можно найти на сайте www.rankingdigitalrights.org.

Дополнительную информацию о проекте New America можно найти на сайте https://www.newamerica.org/.

Дополнительную информацию об Институте открытых технологий (Open Technology Institute) можно найти на сайте https://www.newamerica.org/oti/.

По этой ссылке можно ознакомиться с полным списком спонсоров и партнеров проекта: https://rankingdigitalrights.org/who/partners/.

## Содержание

## 1. О проекте «Рейтинг цифровых прав»

«Рейтинг цифровых прав» (Ranking Digital Rights, RDR) поддерживает принципы свободы самовыражения и приватности в Интернете путем создания международных норм и мер стимулирования компаний по соблюдению и защите прав пользователей. Для этого мы составляем Индекс ответственности корпораций, который оценивает самые влиятельные цифровые платформы и телекоммуникационные компании мира на предмет выполнения ими соответствующих обязательств и политик, основанных на международных стандартах в области защиты прав человека. Мы работаем с компаниями, а также с правозащитниками, исследователями, инвесторами и политиками для установления и поддержания общемировых стандартов корпоративной ответственности.

Компаниям, для которых соблюдение и защита прав человека является приоритетом, Индекс ответственности корпораций RDR предлагает «дорожные карты» по созданию и эксплуатации интернет-платформ и сервисов. Индекс RDR 2019 года оценивает 24 компании по 35 показателям[1]. В рамках открытого [анг] методологического анализа применяется семиэтапный исследовательский процесс [анг]. При проведении анализа рассматриваются управленческие механизмы компаний для выявления и предотвращения потенциальных рисков в отношении соблюдения прав человека пользователей, а также учитывается политика компаний, влияющая на свободу самовыражения и неприкосновенность частной жизни пользователей.

## 2. О методологии Индекса RDR

В основе стандартов, по которым Индекс RDR оценивает компании, лежит опыт более десяти лет работы профессиональных сообществ, занимающихся вопросами защиты прав человека, неприкосновенности частной жизни и информационной безопасности. Стандарты включают Руководящие принципы предпринимательской деятельности в аспекте прав человека ООН, которые утверждают принцип равной ответственности как правительств, так и компаний в области защиты прав человека.

Индекс RDR также опирается на принципы и директивы Глобальной сетевой инициативы (Global Network Initiative), в которых рассматриваются конкретные обязанности ИКТ-компаний в отношении свободы самовыражения и неприкосновенности частной жизни в ситуации, когда правительство предъявляет требования на ограничение контента или передачу информации о пользователях. В то

[1] См. Индекс RDR за 2019 год, https://rankingdigitalrights.org/index2019/ [анг]

же время Индекс опирается на развивающиеся общемировые стандарты и нормы в области защиты данных, информационной безопасности и доступа к информации.

Методология Индекса RDR разрабатывалась в течение многих лет исследований, тестирований и консультаций. С момента своего создания проект тесно сотрудничает с исследователями по всему миру. Для разработки первоначальной модели методологии, проведения пилотного исследования и создания первого индекса RDR мы сотрудничали с компанией Sustainalytics, занимающей лидирующие позиции по проведению исследований в области окружающей среды, социальной сферы и управления для инвесторов.

Предыдущие версии Индекса RDR:

- В 2015 году мы выпустили первый Индекс RDR, в котором 16 интернет- и телекоммуникационных компаний ранжировались по 31 показателю.

- Индекс RDR 2017 года включал в себя уже 22 компании: все компании из рейтинга 2015 года и шесть новых компаний. Наряду с интернет- и телекоммуникационными компаниями в Индекс RDR попали новые виды сервисов, производящих программное обеспечение и устройства, которые мы называем «мобильными экосистемами». В результате детального анализа исходных данных Индекса RDR 2015 года, а также консультаций с заинтересованными сторонами из гражданского общества, научных кругов, инвесторов и компаний мы пересмотрели методологию 2017 года.

- В Индексе RDR 2018 года применялась та же методология для оценки тех же 22 компаний, что и в Индексе 2017 года. Это позволило нам провести сравнительный анализ результатов деятельности каждой компании и проследить общие тенденции.

- В рамках методологии Индекса RDR 2019 года были внесены изменения в два показателя категории «Корпоративное управление»[2]. Эти изменения были направлены на введение базовых стандартов для выявления и снижения рисков в области соблюдения прав человека, связанных с использованием компаниями алгоритмов, а также политики и практики таргетированной рекламы. Мы также пересмотрели один индикатор (G6), чтобы усилить и усовершенствовать оценку применяемых компаниями механизмов и процедур

[2] «Индикаторы исследования Индекса ответственности корпораций», *Ranking Digital Rights*, сентябрь 2019 года, https://rankingdigitalrights.org/index2019/assets/static/download/RDRindex2019indicators.pdf [анг]

рассмотрения жалоб и правовой защиты[3]. Кроме того, Индекс RDR 2019 года пополнился двумя новыми компаниями[4] (Deutsche Telekom и Telenor) и пятью дополнительными облачными сервисами.

## 3. К вопросу о пересмотре методологии Индекса RDR 2020 года

С момента первого выпуска в 2015 году Индекс RDR способствовал улучшению показателей компаний по предоставлению информации о политике и практиках в ряде областей, включая предоставление отчетности о прозрачности, удалении контента, ограничении учетных записей, блокировке работы сетей, а также об обработке и защите пользовательской информации. Однако, учитывая произошедшие за эти годы геополитические и технологические изменения с их явным воздействием на сферу области прав человека, стало ясно, что методология нуждается в обновлении, чтобы компании несли полную ответственность за целый ряд потенциальных онлайн-угроз в области соблюдения прав человека.

В январе 2019 года RDR приступил к процессу по расширению и корректировке методологии с целью включения новых проблемных сфер и новых типов компаний[5]. Эта работа была сосредоточена на трех основных направлениях:

- **Совершенствование методологии индекса RDR 2019 года.** Мы проанализировали методологию индекса RDR 2019 года, чтобы определить ключевые области для пересмотра и улучшения.

- **Включение новых показателей по таргетированной рекламе и алгоритмам.** С начала 2019 года RDR разрабатывает новые показатели, задающие общие стандарты подотчетности и прозрачности в отношении демонстрации компаниями уважительного отношения к правам человека в Интернете по мере разработки и внедрения новых технологий. В октябре 2019 года RDR опубликовал предварительные показатели по таргетированной рекламе и алгоритмам [анг]. Работа основывалась на внутреннем исследовании, которое длилось почти год и учитывало отзывы более 90 экспертов. Предварительные варианты показателей прошли пилотное тестирование исследовательской группой RDR. Результаты пилотного исследования были опубликованы в марте 2020 года [анг].

---

[3] «Предложенные изменения к Индексу ответственности корпораций за 2019 год (предварительный вариант)», *Ranking Digital Rights,* июль 2018 года https://rankingdigitalrights.org/wp-content/uploads/2018/06/2019-Index-Methodology_-Consultation-Draft.pdf [анг]

[4] См. список компаний: https://rankingdigitalrights.org/2019-companies/ [анг]

[5] «Выпуск Индекса RDR 2019 запланирован на май, большие планы», *Ranking Digital Rights,* февраль 2019 года, https://rankingdigitalrights.org/2019/02/13/rdr-2019-index-launch-plans/ [анг]

- **Включение новых компаний.** В начале 2019 года мы начали процесс изучения вопроса о способах дальнейшего расширения Индекса RDR за счет включения в него компаний Amazon и Alibaba. Этот процесс заложил основу для включения двух новых видов сервисов — платформ электронной коммерции и «экосистем персональных цифровых помощников» — в систему методологии Индекса RDR 2020 года.

В апреле 2020 года RDR опубликовал черновой вариант финального Индекса RDR-2020, который объединил работу по трем направлениям[6]. Затем мы провели заключительный цикл общественных консультаций с целью получения ключевой оценки от всех заинтересованных сторон. Это позволило нам принять окончательные решения при доработке методологии.

> Ознакомиться с кратким изложением основных изменений в методологии Индекса RDR за 2020 год можно по этой ссылке: https://rankingdigitalrights.org/wp-content/uploads/2020/06/2020-methodology-revision-final-summary.pdf
>
> Узнать больше о процессе разработки методологии можно по этой ссылке: https://rankingdigitalrights.org/methodology-development/.

## 4. Компании, включенные в Индекс RDR-2020

Индекс RDR за 2020 год оценивает 26 перечисленных ниже компаний. Исследователи изучилили политику и практики «материнской» компании, а также обнародованные политики и практики отдельных сервисов и/или местных операторов (в зависимости от структуры компании).

**Цифровые платформы.** Индекс RDR-2020 оценивает 14 цифровых платформ. Сюда входят 12 цифровых платформ, которые мы оценивали до этого, а также две новые компании (Amazon и Alibaba). Как отмечалось выше, в связи с расширением Индекса RDR-2020 за счет включения новых сервисов, предлагаемых Amazon и Alibaba — в

[6] «Предварительная версия Индекса корпоративной ответственности 2020», *Ranking Digital Rights,* апрель 2020 года, https://rankingdigitalrights.org/wp-content/uploads/2020/04/2020-draft-methodology-redline-version.pdf [анг]

частности, платформ электронной коммерции и экосистем персональных цифровых помощников — мы переименовали категорию «Экосистемы мобильных услуг и интернета» в «Цифровые платформы». К этой категории относится целый ряд продуктов и сервисов, предлагаемых интернет-компаниями, а также экосистемы мобильных устройств, платформы электронной коммерции и экосистемы персональных цифровых помощников.

Опираясь на соответствующие показатели, мы оцениваем глобальную политику каждой из групп компаний, а также политику компаний на их внутреннем рынке. (Пример: мы оцениваем политику приватности Facebook, применимую к пользователям в США).

В рамках анализа деятельности каждой компании мы рассматриваем не более пяти продуктов и сервисов:

- **Alibaba (Китай)** — Taobao.com (платформа электронной коммерции), AliGenie (экосистема персонального цифрового помощника)
- **Amazon (США)** — Amazon.com (платформа электронной коммерции), Amazon Alexa (экосистема персонального цифрового помощника), Amazon Drive
- **Apple (США)** — мобильная экосистема iOS, iMessage, iCloud
- **Baidu (Китай)** — Baidu Search, Baidu Cloud, Baidu PostBar
- **Facebook (США)** — Facebook, Instagram, WhatsApp, Messenger
- **Google (США)** — Search, Gmail, Youtube, мобильная экосистема Android, Google Drive
- **Kakao (Южная Корея)** — Kakao Search, Kakao Mail, KakaoTalk
- **Mail.Ru (Россия)** — ВКонтакте, почта Mail.ru, облачные сервисы Mail.Ru Cloud
- **Microsoft (США)** — Bing, Outlook.com, Skype, OneDrive
- **Oath (США)** — Yahoo Mail, Tumblr
- **Samsung (Южная Корея)** — версия Android для Samsung, Samsung Cloud
- **Tencent (Китая)** — QZone, QQ, WeChat, Tencent Cloud
- **Twitter (США)** — Twitter
- **Яндекс (Россия)** — почта Яндекс, поисковик Яндекс, Диск (облачное хранилище) Яндекс

**Телекоммуникационные компании.** В Индекс RDR 2020 года включены 12 телекоммуникационных компаний, которые мы оценивали ранее. Индекс не содержит ни одной новой телекоммуникационной компании.

Опираясь на соответствующие показатели, мы оцениваем политику каждой компании на уровне всей группы, предоплатные и постоплатные услуги мобильной связи, а также услуги стационарного широкополосного Интернета, если таковые предлагаются:

- **América Móvil (Мексика)**: Telcel (пред- и постоплатные услуги мобильной связи)
- **AT&T (США)**: AT&T (пред- и постоплатные услуги мобильной связи, широкополосный интернет)
- **Axiata (Малайзия):** Celcom (пред- и постоплатные услуги мобильной связи, широкополосный интернет)
- **Bharti Airtel (Индия):** Airtel India (пред- и постоплатные услуги мобильной связи, широкополосный интернет)
- **Deutsche Telekom AG (Германия)**: Deutsche Telekom (пред- и постоплатные услуги мобильной связи, широкополосный интернет)
- **Etisalat (ОАЭ):** Etisalat UAE (пред- и постоплатные услуги мобильной связи, широкополосный интернет)
- **MTN (ЮАР):** MTN South Africa (пред- и постоплатные услуги мобильной связи, широкополосный интернет)
- **Ooredoo (Катар):** Ooredoo Qatar (пред- и постоплатные услуги мобильной связи, широкополосный интернет)
- **Orange (Франция):** Orange France (пред- и постоплатные услуги мобильной связи, широкополосный интернет)
- **Telefónica (Испания):** Movistar (пред- и постоплатные услуги мобильной связи, широкополосный интернет)
- **Telenor ASA (Норвегия):** Telenor (пред- и постоплатные услуги мобильной связи, широкополосный интернет)
- **Vodafone (Великобритания):** Vodafone UK (пред- и постоплатные услуги мобильной связи, широкополосный интернет)

## 5. Порядок проведения исследования

Индекс RDR составляется с использованием строгого, состоящего из семи этапов процесса поиска, перекрестной проверки и анализа данных. В работе задействованы более 30 исследователей со всего мира. Ниже представлены этапы составления индекса RDR за 2020 год.

- **Этап 1: сбор первичных данных.** На этом этапе исследователи, проводящие первичные исследования, отвечают за проверку результатов предыдущего Индекса RDR (за 2019 год) . Если политика компании изменилась или появились новые показатели и составляющие, первичные исследователи

отвечают за проведение их анализа. Исследователи также оценивают, насколько (текущая) политика сопоставима с предыдущим Индексом RDR.

- **Этап 2: вторичный обзор**. На этом этапе аналитики второго цикла проводят оценку фактов оценки первичных исследователей и предоставляют согласие или несогласие с результатами сравнительного анализа.

- **Этап 3: обзор и согласование**. Команда RDR обсуждает результаты, полученные на этапах 1 и 2, и принимает решение по всем возможным разногласиям.

- **Этап 4: обратная связь с компаниями**. На этом этапе у компаний есть возможность ознакомиться с предварительной оценкой и предоставить своей отзыв команде RDR. Команда изучает полученную от компаний информацию и определяет, является ли она основанием для внесения изменений в оценку.

- **Этап 5: обработка отзывов компаний.** RDR рассматривает отзывы компаний и при необходимости вносит коррективы в оценку.

- **Этап 6: горизонтальная оценка.** Команда RDR проводит горизонтальный обзор, используя собранные на этапе 4 отзывы компаний и перекрестную проверку показателей, чтобы удостовериться, что в отношении каждой компании использовался единый метод оценки.

- **Этап 7: окончательная оценка.** Команда RDR выставляет итоговые баллы и заключает, изменилась ли политика компании или уровень обнародованной информации по сравнению с данными предыдущего года.

## 6. Оценка и подсчет баллов

В рамках Индекса RDR за 2020 год оцениваются политики компаний, действовавшие с 25 января 2019 года по 14 сентября 2020 года. Компании получают суммарную оценку своей деятельности по всем категориям Индекса RDR. Результаты показывают, как компании проявили себя по каждой категории и каждому показателю.

Каждый показатель имеет перечень параметров, и компании получают оценку (полную, частичную или нулевую) за каждый соблюденный параметр. Оценка учитывает степень раскрытия информации по каждому параметру показателя, основываясь на одном из следующих возможных ответов:

- **«Да»** (полное раскрытие): раскрытие информации соответствует требованию показателя.
- **«Частичное»**: компания раскрыла некоторые, но не все аспекты данного показателя, или раскрытие не является достаточно полным, чтобы отвечать всем требованиям показателя.
- **«Нет данных о раскрытии информации»**: исследователи не смогли найти на сайте компании информацию, отвечающую на вопрос элемента.
- **«Нет»**: информация существует, но в ней конкретно не раскрывается тематика запроса по данному параметру. Этот вариант отличается от варианта «Раскрытие информации не найдено», хотя оба они не дают положительной оценки.
- **«Неприменимо»**: элемент не имеет отношения к компании или услуге. Элементы, отмеченные как «Неприменимо», не будут учитываться при подсчете баллов как за, так и против.

**Баллы**

- Да/полное раскрытие информации = 100
- Частичное раскрытие информации = 50
- Информация не раскрыта = 0
- Нет данных о раскрытии информации = 0
- Неприменимо - данные не учитываются при подсчете баллов и усредненных значений.

## Корпоративное управление

Показатели данной категории призваны продемонстрировать наличие в компании процессов управления, обеспечивающих соблюдение прав человека на свободу самовыражения и неприкосновенность частной жизни. Данные права закреплены во Всеобщей декларации прав человека[7] и в Международном пакте о гражданских и политических правах[8]. Они действуют как в Интернете, так и за его пределами[9]. Для того чтобы компания показала высокие результаты в этой категории, раскрываемая ею информация о своей деятельности должна как минимум отражать, а в идеале превосходить Руководящие принципы предпринимательской деятельности в сфере прав человека ООН[10] и другие стандарты в области соблюдения прав человека, направленные на обеспечение свободы самовыражения и неприкосновенности частной жизни, принятые Глобальной сетевой инициативой[11].

### G1. Политика принятия обязательств

Компания должна опубликовать официальное заявление о принятии на себя обязательств по соблюдению прав человека в отношении свободы самовыражения, информации и неприкосновенности частной жизни пользователей.

*Параметры:*

1. Принимает ли компания открытые, четко сформулированные обязательства по соблюдению прав человека, включая право на свободу самовыражения и информации?
2. Принимает ли компания открытые, четко сформулированные обязательства по соблюдению прав человека, включая право на приватность?
3. Принимает ли компания открытые, четко сформулированные обязательства по соблюдению прав человека в области разработки алгоритмических систем?

---

[7] Всеобщая декларация прав человека, https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml

[8] Международный пакт о гражданских и политических правах, *Управление Верховного комиссара ООН по правам человека*, https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

[9] Совет ООН по правам человека, *Резолюция, принятая Советом по правам человека 27 июня 2016 года - Поощрение и защита всех прав человека, гражданских, политических, экономических, социальных и культурных прав, включая право на развитие,* https://daccess-ods.un.org/TMP/2969264.09006119.html [анг]

[10] Руководящие принципы предпринимательской деятельности в аспекте прав человека, *Управление Верховного комиссара ООН по правам человека.* https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_ru.pdf

[11] Принципы Глобальной сетевой инициативы, *Global Network Initiative*, https://globalnetworkinitiative.org/gni-principles/ [анг]

**Разъяснения по показателю**

Настоящий показатель призван продемонстрировать, что компания взяла на себя четкие программные обязательства в отношении соблюдения прав человека на свободу самовыражения и информации, а также неприкосновенность частной жизни. Эти стандарты изложены в пункте 16 Руководящих принципов предпринимательской деятельности в аспекте прав человека ООН. Пункт гласит, что компании должны проводить официальную политику, публично подтверждая свою приверженность международным принципам и стандартам в области прав человека[12]. Компании также должны опубликовать формальное заявление о принятии на себя обязательств по соблюдению прав человека при разработке и внедрении систем алгоритмического принятия решений в соответствии с рекомендациями Совета Европы в его Рекомендации о воздействии алгоритмических систем на права человека (2020). Компания должна четко раскрыть эти обязательства в официальных программных документах или других информационных сообщениях, отражающих официальную политику компании.

**Потенциальные источники:**

- Политика компании в области прав человека;
- Отчеты, доклады или любые другие заявления компании, отражающие ее официальную политику;
- Ежегодный отчет компании или отчет компании об устойчивом развитии;
- Политика компании о принципах использования искусственного интеллекта.

### G2. Контроль и надзор со стороны руководства компании

Высшее руководство компании должно осуществлять надзор за тем, как политика и практические действия компании влияют на свободу самовыражения и информации, а также на неприкосновенность частной жизни.

*Параметры:*

1. Предоставляет ли компания четкую информацию о том, что совет директоров осуществляет официальный надзор за тем, как деятельность компании влияет на свободу самовыражения и информации?

[12] Руководящие принципы предпринимательской деятельности в аспекте прав человека, *Управление Верховного комиссара ООН по правам человека* https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_ru.pdf

2. Предоставляет ли компания четкую информацию о том, что совет директоров осуществляет официальный надзор за тем, как деятельность компании влияет на приватность?
3. Предоставляет ли компания четкую информацию о том, что за деятельностью компании, которая влияет на свободу самовыражения и информации, осуществляется надзор со стороны исполнительного комитета, коллектива, целевой программы или ответственного лица высшего руководящего уровня?
4. Предоставляет ли компания четкую информацию о том, что за деятельностью компании, которая влияет на приватность, осуществляется надзор со стороны исполнительного комитета , коллектива, целевой программы или ответственного лица высшего руководящего уровня?
5. Предоставляет ли компания четкую информацию о том, что за деятельностью компании, которая влияет на свободу самовыражения и информации, осуществляется надзор со стороны исполнительного комитета, коллектива, целевой программы или ответственного лица из управленческого звена?
6. Предоставляет ли компания четкую информацию о том, что за деятельностью компании, которая влияет на приватность, осуществляется надзор со стороны исполнительного комитета, коллектива, целевой программы или ответственного лица из управленческого звена?

**Разъяснения по показателю**

Этот показатель призван продемонстрировать, насколько эффективно компания осуществляет управление и надзор по вопросам обеспечения свободы самовыражения, информации и неприкосновенности частной жизни на всех уровнях своей деятельности. Компании должны четко продемонстрировать, что высшее руководство - от совета директоров до уровня управления - осуществляет надзор и несет ответственность за реализацию своей политики и практической деятельности, затрагивающей данные права человека.

Чтобы получить максимальную оценку по этому показателю, компании должны четко указать, что на каждом уровне управления (совет директоров, исполнительный и управленческий состав) осуществляется четкий надзор как в плане обеспечения свободы слова и информации, так и в вопросах обеспечения приватности. На уровне правления такой порядок надзора может включать совет директоров или другое публичное указание относительно того, как правление осуществляет надзор за этими вопросами. На уровне ниже совета директоров он может включать в себя подразделение компании, целевую программу или отдельное должностное лицо, которое отчитывается перед исполнительным или руководящим звеном. Такой отдел, программа, группа, сотрудник и т. д. должны особо отметить в своем описании

обязанностей задачи по обеспечению свободы самовыражения и неприкосновенности частной жизни.

**Потенциальные источники:**
- Список членов совета директоров,
- Учредительные документы компании,
- Отчет компании об устойчивом развитии,
- Организационная структура компании,
- Политика компании в области прав человека,
- Документы о членстве в Global Network Initiative (если компания состоит в этой организации).

### G3. Применение во внутренней политике

Компания должна иметь действующие механизмы реализации своих обязательств по свободе самовыражения, информации и приватности.

*Параметры:*

1. Предоставляет ли компания четкую информацию о проведении обучения сотрудников по вопросам свободы самовыражения и информации?
2. Предоставляет ли компания четкую информацию о проведении обучения сотрудников по вопросам приватности?
3. Предоставляет ли компания четкую информацию о программах для информаторов и механизмах, с помощью которых сотрудники могут докладывать о проблемах, связанных с тем, как компания относится к свободе самовыражения и информационным правам своих пользователей?
4. Предоставляет ли компания четкую информацию о программах для информаторов и механизмах, с помощью которых сотрудники могут докладывать о проблемах, связанных с тем, как компания относится к праву на приватность своих пользователей?

**Разъяснения по показателю**

Предыдущий показатель (G2) оценивает, обязуется ли высшее руководство компании контролировать вопросы свободы самовыражения и приватности. В данном же показателе (G3), оценивается, раскрывает ли компания информацию о том, насколько и как эти обязательства институционализированы в компании. В частности, этот показатель направлен на выявление того, помогает ли компания сотрудникам понять важность свободы самовыражения и неприкосновенности частной жизни. Когда сотрудники пишут компьютерный код для нового продукта, рассматривают запросы на получение пользовательских данных или отвечают на вопросы клиентов о том, как

пользоваться услугами, их действия могут непосредственно влиять на право пользователя на свободу самовыражения и неприкосновенность частной жизни. Мы ожидаем, что компании будут раскрывать информацию о том, проводят ли они обучение, информирующее сотрудников об их роли в соблюдении прав человека и предоставляющее сотрудникам возможность высказывать свои замечания и соображения по поводу соблюдения данных прав.

Компания может получить высокую оценку по этому показателю только в том случае, если она четко раскрывает информацию об обучении сотрудников по вопросам обеспечения свободы слова и информации, неприкосновенности частной жизни, а также о наличии программ по работе с информаторами, сообщающими о нарушениях, касающихся этих вопросов. В отчетности должно быть указано, что в программах по обучению сотрудников и по работе с информаторами содержатся указания на обеспечение свободы слова и защиты частной жизни. Компании также могут получить положительную оценку по этому показателю, если в программе компании по информированию о нарушениях не содержится конкретного указания о подаче жалоб, связанных со свободой самовыражения и неприкосновенностью частной жизни, при условии, что компания взяла на себя обязательства по соблюдению этих принципов в каком-либо другом источнике и способом, дающим возможность четко понять, что компания будет рассматривать эти жалобы в рамках своей программы по информированию о нарушениях.

**Потенциальные источники:**

- Кодекс поведения компании,
- Руководство для сотрудников,
- Организационная структура компании,
- Отчет о социальной ответственности или об устойчивом развитии компании,
- Записи в блоге компании.

### G4: Оценка надлежащего контроля за соблюдением прав человека

### G4(a). Оценка воздействия: Органы власти и нормативные акты

В целях выявления того, как государственные нормативные акты и политика влияют на
свободу самовыражения и информации и на неприкосновенность частной жизни пользователей, а также для предотвращения возможных негативных последствий, возникающих в результате такого влияния в юрисдикциях, в которых компания осуществляет свою деятельность, компаниям следует проводить регулярную

всестороннюю и достоверную процедуру надлежащего контроля, в том числе посредством проведения тщательной экспертизы воздействия на права человека.

*Параметры:*

1. Осуществляет ли компания оценку того, как местное законодательство влияет на соблюдение свободы самовыражения и информации в юрисдикциях, где она ведет свою деятельность?
2. Осуществляет ли компания оценку того, как местное законодательство влияет на соблюдение приватности в юрисдикциях, где она ведет свою деятельность?
3. Осуществляет ли компания оценку рисков в сфере свободы самовыражения и информации в отношении уже имеющихся продуктов и сервисов в юрисдикциях, где компания ведет свою деятельность?
4. Осуществляет ли компания оценку рисков в сфере приватности в отношении уже имеющихся продуктов и сервисов в юрисдикциях, где компания ведет свою деятельность?
5. Оценивает ли компания возможные угрозы в отношении свободы слова и информации, связанные с новым видом деятельности, включая запуск и/или создание новых продуктов, сервисов или компаний, а также выход на новые рынки или юрисдикции?
6. Осуществляет ли компания оценку рисков приватности, связанных с новой деятельностью, включая запуск и/или создание новых продуктов, сервисов или компаний, а также выход на новые рынки или юрисдикции?
7. Проводится ли в компании процедура дополнительной экспертизы в тех случаях, когда в результате проведения оценки рисков выявлены проблемные моменты?
8. Рассматривают ли высшие руководители и/или члены совета директоров компании результаты оценок и комплексной проверки и учитывают ли они их при принятии решений?
9. Проводит ли компания подобные проверки на регулярной основе?
10. Обеспечивается ли проведение оценок независимой сторонней организацией?
11. Является ли независимая сторонняя организация, обеспечивающая проведение экспертизы, заслуживающей доверия организацией, аккредитованной согласно соответствующему авторитетному стандарту в области прав человека?

**Разъяснения по показателю**

Данный показатель отражает, насколько ответственно и систематично компании проводят оценку рисков в области прав человека, связанных с государственными нормативными актами и политикой в юрисдикциях, в которых они работают. Эти аналитические оценки должны являться важной частью официальной, систематизированной деятельности компании по обеспечению должной осмотрительности для гарантирования того, что принимаемые компанией решения и практические действия не приведут к возникновению, способствованию или усугублению негативных последствий в области соблюдения прав человека. Проведение такой экспертизы позволяет компаниям выявлять возможные факторы риска в отношении обеспечения права пользователей на свободу самовыражения и неприкосновенность частной жизни, а также своевременно принимать меры по снижению возможного причиненного вреда в случае выявления такового.

Данный показатель не предполагает, что компании будут публиковать подробные результаты проведенных ими оценок воздействия на соблюдение прав человека, поскольку подобные данные могут содержать конфиденциальную информацию. Напротив, ожидается, что компании должны обнародовать информацию о том, что они проводят оценку воздействия на права человека (ОВПЧ), а также предоставить информацию о том, что включает в себя их процесс ОВПЧ.

**Потенциальные источники:**

- Отчет о социальной ответственности/устойчивом развитии компании,
- Политика компании в области прав человека,
- Отчет о соответствии стандартам Global Network Initiative.

**G4(b). Оценка воздействия: Процессы применения политики**

Для выявления влияния реализации политики компании на ключевые права пользователей в области свободы самовыражения и информации, приватности, недопустимости дискриминации, а также для предотвращения возникновения возможных негативных последствий необходимо проводить регулярную всестороннюю и достоверную процедуру комплексной проверки, в частности посредством проведения тщательной оценки воздействия на права человека, и принимать соответствующие меры по предупреждению возможных последствий.

*Параметры:*

1. Проводит ли компания оценку рисков, связанных с обеспечением свободы самовыражения и информации при применении ее условий предоставления услуг?

2. Проводит ли компания оценку рисков, связанных с обеспечением приватности при применении ее условий предоставления услуг?
3. Оценивает ли компания дискриминационные риски, связанные с ее механизмами применения условий предоставления услуг?
4. Оценивает ли компания дискриминационные риски, связанные с ее механизмами применения политики приватности?
5. Проводится ли в компании процедура дополнительной экспертизы в тех случаях, когда в результате проведения оценки рисков выявлены проблемные моменты?
6. Рассматривают ли руководители высшего звена и/или члены совета директоров компании результаты оценок и комплексной проверки и учитывают ли их при принятии решений?
7. Проводит ли компания подобные проверки на регулярной основе?
8. Обеспечивается ли проведение проверок независимой сторонней организацией?
9. Является ли независимая сторонняя организация, обеспечивающая проведение экспертизы, заслуживающей доверия организацией, аккредитованной согласно соответствующему авторитетному стандарту в области прав человека?

**Разъяснения по показателю**

Показатель отражает, насколько ответственно и систематично компании проводят оценку рисков в области прав человека, связанных с воздействием их собственной политики на фундаментальные права пользователей на свободу самовыражения, неприкосновенность частной жизни и недискриминацию. Эти аналитические оценки должны являться важной частью официальной систематизированной деятельности компании по обеспечению должной осмотрительности для гарантирования того, что принимаемые компанией решения и практические действия не приведут к возникновению, способствованию или усугублению негативных последствий в области соблюдения прав человека. Проведение такой экспертизы позволяет компаниям выявлять возможные факторы риска в отношении обеспечения права пользователей на свободу самовыражения и неприкосновенность частной жизни, а также своевременно принимать меры по снижению возможного причиненного вреда в случае выявления такового.

Данный показатель не предполагает, что компании будут публиковать подробные результаты проведенных ими оценок воздействия на соблюдение прав человека, поскольку подобные данные могут содержать конфиденциальную информацию.

Ожидается, что компании обнародуют факт проведения ОВПЧ и предоставят информацию о том, что включает в себя их процесс ОВПЧ.

**Потенциальные источники:**

- Отчет о социальной ответственности/устойчивом развитии компании,
- Политика компании в области прав человека,
- Отчет о соответствии стандартам Global Network Initiative.

**G4(c) Оценка воздействия: Таргетированная реклама**

В целях выявления того, как различные аспекты использования таргетированной рекламы влияют на фундаментальные права на свободу самовыражения и информации, недопустимость дискриминации и неприкосновенность частной жизни пользователей, а также для предотвращения возможных негативных последствий, возникающих в результате такого влияния, компаниям следует проводить регулярную всестороннюю и достоверную процедуру комплексной проверки, в частности посредством проведения тщательной оценки воздействия на права человека.

*Параметры:*

1. Осуществляет ли компания оценку рисков свободы самовыражения и информации, связанных с ее политикой и деятельностью в области таргетированной рекламы?
2. Осуществляет ли компания оценку рисков приватности, связанных с ее политикой и деятельностью в области таргетированной рекламы?
3. Оценивает ли компания дискриминационные риски, связанные с ее политикой и деятельностью в области таргетированной рекламы?
4. Проводится ли в компании процедура дополнительной экспертизы в тех случаях, когда в результате проведения оценки рисков выявлены проблемные моменты?
5. Рассматривают ли руководители высшего звена и/или члены совета директоров компании результаты оценок и комплексной проверки и учитывают ли их при принятии решений?
6. Проводит ли компания подобные проверки на регулярной основе?
7. Обеспечивается ли проведение проверок независимой сторонней организацией?
8. Является ли независимая сторонняя организация, обеспечивающая проведение экспертизы, заслуживающей доверия организацией, аккредитованной согласно соответствующему авторитетному стандарту в области прав человека?

**Разъяснения по показателю**

Таргетированная реклама может оказывать негативное воздействие на соблюдение прав человека, в частности на права пользователей на свободу информации, свободу информации и защиту от дискриминации[13]. Дискриминация возникает, когда платформы позволяют сторонним рекламодателям показывать разную рекламу разным пользователям на основе открытой или предположительной информации, включая принадлежность к социально защищенным категориям (раса, этническая принадлежность, возраст, гендерная самоидентификация и самовыражение, сексуальная ориентация, состояние здоровья, наличие инвалидности и т. д.). Дискриминация может не быть противозаконной или непосредственно пагубной, чтобы привести к отрицательным последствиям в масштабе, например, на уровне населения или за период жизни отдельного человека. Принимая во внимание тот факт, что таргетированная реклама менее прозрачна, чем другие формы рекламы, а также учитывая наличие у компаний значительных финансовых мотиваций для быстрого внедрения данной технологии, этот потенциальный урон правам человека необходимо учитывать при оценке рисков.

Данный показатель отражает, насколько ответственно и систематично компании проводят оценку рисков в области прав человека, связанных с воздействием таргетированной рекламы на фундаментальные права пользователей на свободу самовыражения, неприкосновенность частной жизни и недискриминацию. Эти аналитические оценки должны являться важной частью официальной систематизированной деятельности компании по обеспечению процедуры комплексной проверки, гарантирующей, что принимаемые компанией решения и практические действия не приведут к возникновению, способствованию или усугублению негативных последствий в области соблюдения прав человека. Проведение такой экспертизы позволяет компаниям выявлять возможные факторы риска в отношении обеспечения права пользователей на свободу самовыражения и неприкосновенность частной жизни при применении политики компании и ее действий в области таргетированной рекламы, а также своевременно принимать меры по снижению возможного причиненного ущерба в случае выявления такового.

Данный показатель не предполагает, что компании будут публиковать подробные результаты проведенных ими оценок воздействия на соблюдение прав человека,

[13] «Сценарии угроз правам человека: таргетированная реклама», *Ranking Digital Rights*, февраль 2019 года, https://rankingdigitalrights.org/wp-content/uploads/2019/02/Human-Rights-Risk-Scenarios-targeted-advertising.pdf [анг].

поскольку подобные данные могут содержать конфиденциальную информацию. Ожидается, что компании обнародуют факт проведения ОВПЧ и предоставят информацию о том, что включает в себя их процесс ОВПЧ.

**Потенциальные источники:**

- Отчет о социальной ответственности/устойчивом развитии компании,
- Политика компании в области прав человека,
- Отчет о соответствии стандартам Global Network Initiative.

### G4(d). Оценка воздействия: Алгоритмические системы

В целях выявления того, как различные аспекты использования алгоритмических систем влияют на ключевые права на свободу самовыражения, свободу информации, недопустимость дискриминации и неприкосновенность частной жизни пользователей, а также для предотвращения возможных негативных последствий, возникающих в результате такого влияния, компаниям следует проводить регулярную всестороннюю и достоверную процедуру комплексной проверки, в частности посредством проведения тщательной экспертизы воздействия на права человека.

*Параметры:*

1. Осуществляет ли компания оценку рисков свободы самовыражения и информации, связанных с ее политикой и деятельностью в области алгоритмических систем?
2. Осуществляет ли компания оценку рисков в сфере приватности, связанных с ее политикой и деятельностью в области алгоритмических систем?
3. Оценивает ли компания дискриминационные риски, связанные с разработкой и использованием алгоритмических систем?
4. Проводится ли в компании процедура дополнительной экспертизы в тех случаях, когда в результате проведения оценки рисков выявлены проблемные моменты?
5. Рассматривают ли руководители высшего звена и/или члены совета директоров компании результаты оценок и комплексной проверки и учитывают ли их при принятии решений?
6. Проводит ли компания подобные проверки на регулярной основе?
7. Обеспечивается ли проведение проверок независимой сторонней организацией?
8. Является ли независимая сторонняя организация, обеспечивающая проведение экспертизы, заслуживающей доверия организацией,

аккредитованной согласно соответствующему авторитетному стандарту в области прав человека?

**Разъяснения по показателю**

Существует целый ряд причин, по которым алгоритмические системы могут нанести урон соблюдению прав человека[14]. Разработка таких систем может использовать информацию о пользователе, часто без ведома или явного, осведомленного согласия со стороны субъекта этих данных, что представляет собой нарушение прав человека на неприкосновенность частной жизни. Подобные системы также могут причинять или способствовать причинению ущерба в сфере свободы самовыражения и распространения информации. Кроме того, целью многих алгоритмических систем принятия решений является автоматизация персонализации пользовательского опыта на основе собранной и смоделированной информации о пользователе, что может способствовать возникновению дискриминации. Поэтому при разработке и использовании в своей деятельности алгоритмических систем компаниям следует проводить оценку рисков в области прав человека в соответствии с Рекомендациями Совета Европы о воздействии алгоритмических систем на права человека (2020 год).

Данный показатель отражает, насколько ответственно и систематично компании проводят оценку рисков в области прав человека, связанных с воздействием алгоритмических систем на фундаментальные права пользователей на свободу самовыражения, неприкосновенность частной жизни и недискриминацию. Эти аналитические оценки должны являться важной частью официальной, систематизированной деятельности компании по обеспечению процедуры комплексной проверки для гарантирования того, что принимаемые компанией решения и практические действия, связанные с разработкой и введением в эксплуатацию алгоритмических систем, не приведут к возникновению, способствованию или усугублению негативных последствий в области соблюдения прав человека. Проведение такой экспертизы позволяет компаниям выявлять возможные факторы риска в отношении обеспечения права пользователей на свободу самовыражения и неприкосновенность частной жизни, а также своевременно принимать меры по снижению возможного причиненного вреда в случае выявления такового.

Данный показатель не предполагает, что компании будут публиковать подробные результаты проведенных ими оценок воздействия на соблюдение прав человека,

[14] «Сценарии угроз правам человека: алгоритмы, машинное обучение и автоматизированное принятие решений», *Ranking Digital Rights*, июль 2019 года, https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-algorithms-machine-learning-automated-decision-making.pdf [анг].

поскольку подобные данные могут содержать конфиденциальную информацию. Ожидается, что компании обнародуют факт проведения ОВПЧ и предоставят информацию о том, что включает в себя их процесс ОВПЧ.

**Потенциальные источники:**

- Отчет о социальной ответственности/устойчивом развитии компании,
- Политика компании в области прав человека,
- Отчет о соответствии стандартам Global Network Initiative.

### G4(e) Оценка воздействия: Нулевой рейтинг

Если в компании применяется практика нулевого рейтинга, ей следует проводить регулярну, всестороннюю и достоверную процедуру комплексной проверки, в частности посредством проведения тщательной экспертизы воздействия на права человека. Целью проверки является определение того, как политика компании в отношениии нулевого рейтинга и все возможные варианты ее использования влияют на ключевые права на свободу самовыражения, свободу информации, недопустимость дискриминации и неприкосновенность частной жизни пользователей, а также для предотвращения возможных негативных последствий, возникающих в результате такого влияния.

*Параметры:*

1. Осуществляет ли компания оценку рисков свободы самовыражения и информации, связанных с ее политикой и деятельностью по применению нулевого рейтинга?
2. Осуществляет ли компания оценку рисков приватности, связанных с ее политикой и деятельностью по применению нулевого рейтинга?
3. Оценивает ли компания дискриминационные риски, связанные с применением применением нулевого рейтинга?
4. Проводится ли в компании процедура дополнительной экспертизы в тех случаях, когда в результате проведения оценки рисков выявлены проблемные моменты?
5. Рассматривают ли руководители высшего звена и/или члены совета директоров компании результаты оценок и комплексной проверки и учитывают ли их при принятии решений?
6. Проводит ли компания подобные проверки на регулярной основе?
7. Обеспечивается ли проведение проверок независимой сторонней организацией?

8. Является ли независимая сторонняя организация, заслуживающей доверия организацией, аккредитованной согласно соответствующему авторитетному стандарту в области прав человека?

**Разъяснения по показателю**

Понятие «нулевой рейтинг» относится к услугам, которые могут предлагаться как телекоммуникационными компаниями, так и платформами в партнерстве с телекоммуникационными компаниями, и которые предоставляют доступ к определенным онлайн-сервисам или платформам независимо от тарифного плана пользователя. Многие телекоммуникационные провайдеры, включая компании, входящие в рейтинг RDR, предлагают такие программы либо в качестве основного поставщика услуги, либо в партнерстве с платформами социальных сетей, например, Free Basics от Facebook. Подобные виды услуг являются формой приоритетного использования сети, что подрывает принципы сетевого нейтралитета и может вызвать ряд других возможных нарушений прав человека, включая ущемление права на свободу самовыражения и информации. Проект Global Voices Advox назвал программу Free Basics от Facebook «механизмом сбора коммерчески выгодных данных пользователей» (Global Voices, 2017), что вызывает серьезные опасения по поводу конфиденциальности этой программы.

Программы нулевого рейтинга также могут носить дискриминирующий характер, отдавая предпочтение определенным типам данных либо на основе соответствующего протокола (HTTP, HTTPS, VoIP и др.), либо на основе контента (отдавая предпочтение одной социальной сети). Дискриминация по типу данных может, в свою очередь, привести к нарушению прав человека на основе изучения персональных данных пользователей, включая пол, расовую или этническую принадлежность, язык (языки), общения и огромное множество других характеристик.

Данный показатель отражает, насколько ответственно и систематично компании проводят оценку рисков в области прав человека, связанных с воздействием применения программ нулевого рейтинга на фундаментальные права пользователей. Компании, предлагающие подобные программы, должны проводить оценки их влияния на фундаментальные права пользователей на свободу самовыражения, неприкосновенность частной жизни и недискриминацию. Эти аналитические оценки должны являться важной частью официальной систематизированной деятельности компании по обеспечению процедуры комплексной проверки для гарантирования того, что принимаемые компанией решения и практические действия не приведут к возникновению, способствованию или усугублению негативных последствий в области соблюдения прав человека. Проведение экспертизы позволяет компаниям выявлять возможные факторы риска, связанные с программами нулевого рейтинга и

своевременно принимать меры по снижению возможного причиненного вреда в случае выявления такового.

Данный показатель не предполагает, что компании будут публиковать подробные результаты проведенных ими оценок воздействия на соблюдение прав человека, поскольку подобные данные могут содержать конфиденциальную информацию. Ожидается, что компании обнародуют факт проведения ОВПЧ и предоставят информацию о том, что включает в себя их процесс ОВПЧ.

**Потенциальные источники:**

- Отчет о социальной ответственности или устойчивом развитии компании,
- Политика компании в области прав человека,
- Отчет о соответствии стандартам Global Network Initiative.

## G5. Взаимодействие с заинтересованными сторонами и подотчетность

Компания должна взаимодействовать с широким кругом заинтересованных сторон по вопросам влияния компании на свободу самовыражения и информации, неприкосновенность частной жизни, а также по проблеме потенциальных рисков причинения вреда в сфере прав человека, в частности, дискриминации.

*Параметры:*

1. Является ли компания членом одной или более многосторонних инициатив, направленных на изучение всевозможных способов воздействия на базовые права пользователей, на свободу самовыражения и информации, неприкосновенность частной жизни и недопущение дискриминации в результате деятельности компании?
2. Если компания не является членом одной или нескольких подобных многосторонних инициатив, является ли компания членом каких-либо организаций, которые систематически и на постоянной основе взаимодействуют с представителями неотраслевых и негосударственных заинтересованных кругов по вопросам защиты свободы самовыражения и неприкосновенности частной жизни?
3. Если компания не является участником ни одной из подобных организаций, предоставляет ли компания сведения об организации или участии во встречах с заинтересованными сторонами, являющимися представителями, правозащитниками лиц или же непосредственно лицами, чьи права на свободу самовыражения и информации, а также на неприкосновенность частной жизни напрямую связаны с деятельностью компании?

**Разъяснения по показателю**

Данный показатель демонстрирует, насколько компания взаимодействует с заинтересованными сторонами и несет перед ними ответственность, в особенности в отношении тех, чья деятельность в Интернете сопряжена с рисками с точки зрения защиты прав человека.

Ожидается, что взаимодействие с заинтересованными сторонами станет основным элементом процессов разработки политики компании и определения ее воздействия. Взаимодействие с заинтересованными сторонами должно осуществляться по всей совокупности вопросов, связанных со свободой слова и информации, защитой частной жизни и другими правами пользователей, включая процесс разработки компанией условий предоставления услуг, политик конфиденциальности и защиты персональных данных, использования алгоритмов, управления таргетированной рекламой, а также практику обеспечения соблюдения этих политик.

Механизмы взаимодействия с заинтересованными сторонами и подотчетности должны включать весь спектр возможных путей нарушения прав пользователей: правительственные требования, действия со стороны третьих лиц, использующих продукты и сервисы компании, или же самих компаний. Для получения максимальной оценки по данному показателю компании должны не только взаимодействовать с заинтересованными сторонами, но и принимать на себя обязательства по обеспечению подотчетности, например, проводить независимые экспертизы под наблюдением какого-либо учреждения, чьи решения не подконтрольны самой компании.

Взаимодействие с заинтересованными сторонами, особенно с теми, кто работает в условиях повышенной опасности, может быть крайне непростым. Может оказаться, что компании не выгодно раскрывать публично детали о том, с какими заинтересованными сторонами она консультируется, где и когда они встречаются и что обсуждают. Тем не менее, мы призываем компании предоставлять нечувствительную информацию о сотрудничестве с другими заинтересованными сторонами. Также мы добиваемся, как минимум, предоставления общественности информации о взаимодействии компании с заинтересованными сторонами, которые сами являются или представляют интересы пользователей, чьи права на свободу выражения мнения и неприкосновенность частной жизни находятся под угрозой.

Один из способов, благодаря которому общественность может быть проинформирована об участии компании в подобном сотрудничестве и о том, что подобное взаимодействие приносит реальные результаты, - это участие компании в

разносторонней общественной инициативе, целью которой является не только создание безопасного пространства для диалога, но и поддержка компаний во взятии на себя обязательств и дальнейшего их исполнения. Полноценные и надежные механизмы подотчетности требуют многостороннего управления, при котором компании не контролируют единолично решения в отношении процессов подотчетности и взаимодействия, а делят полномочия по принятию решений с представителями других заинтересованных сторон.

Если компания получает максимальный балл по 1-му пункту, она автоматически получает максимальный балл по 2-му и 3-му пунктам. Поскольку сфера деятельности Global Network Initiative сосредоточена на работе с правительственными запросами, а как минимум половина методологии RDR затрагивает вопросы защиты прав человека перед угрозами, источником которых не являются правительственные органы, то для индекса RDR 2020 года членство в Global Network Initiative (при отсутствии подтверждения вовлеченности и подотчетности компании в сфере других рисков в области прав человека помимо тех, источником которых являются правительственные структуры) приведет лишь к частичному зачету по пункту 1 данного показателя.

**Потенциальные источники:**

- Отчет о социальной ответственности или устойчивом развитии компании,
- Годовой отчет компании,
- Блог компании,
- Часто задаваемые вопросы или центр поддержки компании.

## G6. Средства правовой защиты и апелляции

### G6(a). Средства правовой защиты

Компания должна иметь понятные и предсказуемые механизмы рассмотрения жалоб и средств правовой защиты для урегулирования жалоб пользователей в связи с нарушением свободы самовыражения и неприкосновенности частной жизни.

*Параметры:*

1. Предоставляет ли компания четкую информацию о наличии механизма(-ов) рассмотрения жалоб, позволяющего(-их) пользователям подавать жалобы, если они считают, что политика или практика компании негативно повлияли на их свободу самовыражения и информационные права?
2. Предоставляет ли компания четкую информацию о наличии механизма(-ов) рассмотрения жалоб, позволяющего(-их) пользователям подавать жалобы,

если они считают, что политика или практика компании негативно повлияла на их частную жизнь?

3. Предоставляет ли компания четкую информацию о порядке предоставления средств правовой защиты в случае жалоб, связанных со свободой слова и информации?
4. Предоставляет ли компания четкую информацию о порядке предоставления средств правовой защиты в случае жалоб, связанных с приватностью?
5. Предоставляет ли компания четкую информацию о сроках рассмотрения жалоб и процедурах правовой защиты?
6. Предоставляет ли компания четкую информацию о количестве полученных жалоб, связанных со свободой самовыражения?
7. Предоставляет ли компания четкую информацию о количестве полученных жалоб, связанных с приватностью?
8. Предоставляет ли компания четкую информацию об обеспечении средствами правовой защиты по жалобам, связанным со свободой самовыражения?
9. Предоставляет ли компания четкую информацию об обеспечении средствами правовой защиты в связи с жалобами на нарушение прав частной жизни?

**Разъяснения по показателю**

Соблюдение и обеспечение защиты прав человека возможно только в том случае, если пользователи имеют возможность получить доступ к средствам правовой защиты, когда считают, что их права были нарушены. Данный показатель отражает, предоставляют ли компании такие механизмы правовой защиты и раскрывают ли они публично данные о порядке реагирования на жалобы лиц, считающих, что компания нарушила или непосредственно способствовала нарушению их свободы самовыражения или неприкосновенности частной жизни.

Предполагается, что компании должны четко предоставлять информацию о механизме рассмотрения жалоб, позволяющем пользователям подавать жалобы, если они считают, что их свобода самовыражения и неприкосновенность частной жизни были нарушены политикой или действиями компании. Чтобы получить максимальную оценку по параметру 1, механизм рассмотрения жалоб компании не обязательно должен прямо указывать, что он применяется именно к жалобам, связанным со свободой самовыражения и неприкосновенностью частной жизни. Однако должно быть совершенно четко указано, что этот механизм может быть использован для подачи любого вида жалоб, связанных с нарушением прав человека. Также предполагается, что механизм подачи жалоб компании должен быть максимально доступным для пользователей. Помимо этого, компания должна подробно разъяснить процедуру предоставления средств правовой защиты по таким видам жалоб и

предоставить свидетельства выполнения подобных процедур. Компании должны описать четкие сроки каждого этапа процесса рассмотрения жалоб и предоставления средств правовой защиты. Эти стандарты изложены в Принципе 31 Руководящих принципов предпринимательской деятельности в аспекте прав человека ООН, который гласит, что компании должны публиковать четкие, доступные и предсказуемые процедуры предоставления средств правовой защиты[15].

**Потенциальные источники:**

- Условия предоставления услуг компании или соответствующие пользовательские соглашения;
- Политика компании в отношении контента;
- Политика компании в сфере защиты персональных данных, руководство по обеспечению защиты персональных данных или информационный ресурс по защите персональных данных;
- Отчет о социальной ответственности или устойчивом развитии компании;
- Центр поддержки компании или руководство пользователя;
- Отчет компании о прозрачности (в зависимости от количества полученных жалоб);
- Рекламная политика компании.

### G6(b). Процесс рассмотрения апелляций на модерацию контента

Компания должна предоставить пользователям понятные и предсказуемые механизмы и порядок обжалования действий по модерации контента.

*Параметры:*

1. Предоставляет ли компания четкую информацию о наличии у затронутых пользователей возможности подачи апелляций на действия по модерации контента?
2. Предоставляет ли компания четкую информацию об оповещении затронутых пользователей о действиях по модерации контента?
3. Предоставляет ли компания четкую информацию о сроках при оповещении затронутых пользователей о действиях по модерации контента?

[15] Руководящие принципы предпринимательской деятельности в аспекте прав человека, *Управление Верховного комиссара ООН по правам человека*, 2011 год, https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_ru.pdf.

4. Предоставляет ли компания четкую информацию о том, в каких случаях обжалование не допускается?
5. Предоставляет ли компания четкое описание процедуры рассмотрения апелляций?
6. Предоставляет ли компания четкое описание сроков рассмотрения апелляций?
7. Указывает ли компания в четкой форме, что подобные апелляции будут рассмотрены как минимум еще одним лицом, не вовлеченным в принятие первоначального решения о модерации контента?
8. Предоставляет ли компания четкую информацию о том, какую роль играет автоматизированный процесс в рассмотрении апелляций?
9. Предоставляет ли компания четкую информацию о том, что пользователи, которых затрагивает данная процедура, получают возможность предоставления дополнительной информации, которая будет учитываться при рассмотрении апелляции?
10. Предоставляет ли компания четкую информацию о предоставлении затронутым пользователям отчета с указанием причины своего решения?
11. Предоставляет ли компания четкие доказательства своей деятельности по рассмотрению апелляций по вопросам модерации контента?

**Разъяснения по показателю**

Независимо от того, насколько четко платформа прописывает условия предоставления услуг, в столь трудоемком и весьма субъективном деле, как модерация контента, неизбежны различные ошибки. В особенности это касается тех случаев, когда процесс модерации контента стремительно масштабируется за счет использования средств автоматизации. Для соблюдения свободы самовыражения и информационных прав пользователей компании должны обеспечить надежную и прозрачную систему подачи апелляций, позволяющую пользователям опротестовывать принимаемые компанией решения, непосредственно влияющие на возможность пользователей осуществлять свои права. Компании должны четко раскрывать механизм обжалования действий по модерации контента, включая предоставление затронутым пользователям возможности немедленной апелляции. Эффективный процесс подачи апелляций должен включать в себя надзор со стороны проверяющего человека и предусматривать возможность предоставления затронутыми пользователями дополнительной информации. Компании также должны предлагать четкие сроки рассмотрения апелляций и четко указывать на случаи и обстоятельства, которые обжалованию не подлежат.

Для получения максимальной оценки по данному показателю компании должны проинформировать пользователей о порядке и способе обжалования и дать подробное описание действий, следующих за поступлением апелляции на рассмотрение. В частности, компания должна уведомить пользователей о возможностях подачи апелляции сразу после того, как компания предпримет первоначальные действия в отношении их контента, разъяснить роль как автоматизированных систем, так и независимых модераторов-людей в процессе рассмотрения поданных апелляций, разъяснить причину принятия решения по соответствующей апелляции и соответствующие ей сроки, а также четко указать случаи и обстоятельства, которые обжалованию не подлежат. Компании также должны четко продемонстрировать, что они реагируют на апелляции, публикуя данные о полученных апелляциях и результатах их рассмотрения.

**Потенциальные источники:**

- Условия предоставления услуг компании или пользовательские соглашения,
- Политики приватности компании,
- Отчет компании об устойчивом развитии.

## Свобода самовыражения и информации

Показатели в данной категории позволяют определить, что компания продемонстрировала уважительное отношение к правам на свободу самовыражения и информации в соответствии с положениями Всеобщей декларации прав человека[16], Международного пакта о гражданских и политических правах[17] и других международных правовых норм в области прав человека. Опубликованные политика и практика компании позволяют наглядно продемонстрировать, какие меры принимаются для противостояния нарушениям в области прав человека, за исключением случаев, когда такие действия являются законными, соразмерными и преследуют оправданную цель. Компании, демонстрирующие высокие результаты по этому показателю, подтверждают свою приверженность принципу открытости не только в том, как они реагируют на требования правительства и других сторон, но и в том, как они устанавливают, разъясняют и соблюдают собственные правила и принципы коммерческой деятельности, влияющие на фундаментальное право пользователей на свободу слова и информации.

### F1: Доступ к политикам

#### F1(a). Доступ к условиям предоставления услуг

Компания должна обеспечить доступ к условиям предоставления услуг, которые можно легко найти и легко понять.

*Параметры:*

1. Легко ли найти условия предоставления услуг компании?
2. Доступны ли условия предоставления услуг на основном языке (-ах), на котором (-ых) говорят пользователи в юрисдикции деятельности компании?
3. Представлены ли условия предоставления услуг в понятной форме?

#### Разъяснения по показателю

Условия предоставления услуг компании определяют взаимоотношения между пользователем и компанией. Эти условия содержат правила относительно

[16] Всеобщая декларация прав человека, https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml

[17] Международный пакт о гражданских и политических правах, *Управление Верховного комиссара ООН по правам человека*, https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

недопустимого контента и запрещенной деятельности; кроме этого компании могут принимать меры в отношении пользователей за нарушение установленных в условиях правил. Поэтому мы ожидаем, что компании обеспечат легкодоступность и понятность данных условий.

С помощью этого показателя можно оценить, насколько легко пользователи могут найти условия предоставления услуг компании. Легкий для поиска документ расположен на главной странице компании или в разделе услуг, на расстоянии одного-двух кликов от главной страницы или в том логически обоснованном месте, где пользователи могут рассчитывать его найти. Использование позиционирования или цветовых схем, которые делают текст или ссылку менее заметными или труднодоступными на веб-странице, означает, что документ не является легкодоступным.

Пользовательское соглашение в приложении не должны быть более чем «в двух кликах» от приложения (например, путем включения опции «Конфиденциальность/Защита данных» в меню приложения). Соглашение также должно быть доступно на основном(-ых) языке(-ах) преимущественного потребительского рынка. Кроме того, мы рассчитываем, что компания предпримет шаги, чтобы способствовать пониманию пользователями информации, представленной в ее документах. Это подразумевает, в частности, предоставление аннотаций, советов или рекомендаций, объясняющих значение терминов, использование заголовков разделов, удобочитаемого размера шрифта или других графических элементов, помогающих пользователям понять документ, а также написание терминов с использованием удобочитаемого синтаксиса.

**Потенциальные источники:**

- Пользовательское соглашение компании, правила использования, правила и условия и др.;
- Политика допустимого использования компании, рекомендации для сообщества, общие правила и др.

**F1(b). Доступ к политике в отношении рекламного контента**

Компания должна обеспечить доступ к политике в отношении рекламного контента, которую можно легко найти и легко понять.

*Параметры:*

1. Легко ли найти политику компании в отношении рекламного контента?

2. Доступна ли политика компании в отношении рекламного контента на основном языке (-ах), на котором (-ых) говорят пользователи в юрисдикции деятельности компании?
3. Представлена ли политика компании в отношении рекламного контента в понятной форме?
4. Для мобильных экосистем: Сообщает ли компания в четкой форме, что в соответствии с ее требованиями к приложениям, доступным через магазин приложений, пользователям должна быть предоставлена политика в отношении рекламного контента?
5. Для экосистем персональных цифровых помощников: Сообщает ли компания в четкой форме, что в соответствии с требованиями к навыкам помощников, доступным через ее магазин навыков, пользователю должна быть предоставлена политика в отношении рекламного контента?

**Разъяснения по показателю**

Компании, предоставляющие возможность размещения всех видов рекламы на своих сервисах или платформах, должны в обязательном порядке указывать, какие виды рекламного контента запрещены - например, реклама, дискриминирующая отдельных лиц или группы лиц по таким признакам как возраст, религия, пол и этническая принадлежность.

Компании должны быть максимально прозрачными в отношении данных правил, чтобы как пользователи, так и рекламодатели имели представление о том, какие типы рекламного контента являются недопустимыми, а также об ответственности за рекламный контент, который появляется на сервисах или платформах компаний.

Поэтому компании должны сделать эти правила легкодоступными для поиска (показатель E1), понятными (показатель E3) и доступными на основных языках на внутреннем рынке компании (показатель E2). Компании, управляющие мобильными экосистемами (Apple iOS, Google Android и реализация Android для Samsung) и экосистемами персональных цифровых помощников (Amazon Alexa, Alibaba AliGenie), должны предоставлять пользователям возможность выбирать, какие приложения или навыки скачиваются с учетом их включенности (или невключенности) в рекламные сети. Поэтому в пунктах 4 и 5 необходимо определить, сообщает ли компания о необходимости предоставления пользователям политики в отношении рекламного контента для приложений или навыков, доступных через ее магазин приложений или магазин навыков.

**Потенциальные источники:**

- Политика компании в отношении рекламного контента,

- Центр компании по помощи предпринимателям,
- Пользовательское соглашение.

**F1(c). Доступ к политике таргетирования рекламы**

Компания должна обеспечить доступ к политике таргетирования рекламы, которую легко найти и легко понять.

*Параметры:*

1. Легко ли найти политику таргетирования рекламы компании?
2. Доступны ли правила таргетирования рекламы на основном языке (-ах), на котором (-ых) говорят пользователи в юрисдикции деятельности компании?
3. Представлена ли политика таргетирования рекламы в понятной форме?
4. Для мобильных экосистем: Сообщает ли компания в четкой форме, что в соответствии с требованиями к приложениям, доступным через ее магазин приложений, пользователям должна быть предоставлена политика таргетирования рекламы?
5. Для экосистем персональных цифровых помощников: Сообщает ли компания в четкой форме, что она требует, чтобы навыки, доступные через ее магазин навыков, предоставляли пользователям политику таргетирования рекламы?

**Разъяснения по показателю**

В дополнение к предоставлению доступной политики рекламного контента (F1b) компании также должны в четкой форме раскрывать свою политику таргетинга рекламы. Возможность рекламодателей или иных третьих сторон ориентировать пользователей на специально подобранный контент на основе их поведения в браузере, информации о местоположении, а также других собранных в их отношении данных и характеристик[18] может существенно изменить (а в некоторых случаях и исказить) экосистему пользователя в Интернете.

Таргетинг, который может включать как платный, так и бесплатный контент, может усиливать социальное неравенство в офлайне и быть откровенно дискриминационным. Он также может привести к так называемым «пузырям фильтров», а также способствовать распространению сомнительного контента, в том числе направленного на введение в заблуждение или распространение ложных

[18] Для получения дополнительной информации о политиках выведения данных см. раздел 6.2 пилотного исследования «2020 Pilot Study and Lessons Learned», *Ranking Digital Rights*, 16 марта 2020 года https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf [анг].

сведений[19]. Поэтому компании, предоставляющие рекламодателям и другим третьим сторонам возможности целевого охвата своих пользователей с помощью специально подобранной рекламы или контента, должны публиковать политику таргетирования: доступную и понятную пользователям, на языках региона деятельности компании. Пользователи должны иметь возможность ознакомления и понимания подобных регламентаций, чтобы принимать информированные решения, полагаясь на полученную ими информацию о рекламном контенте.

Применительно к мобильным экосистемам и экосистемам персональных цифровых помощников компании должны сообщать о требовании к приложениям или навыкам, доступным через их магазины приложений или магазины навыков, предоставлять пользователям информацию о политике таргетирования рекламы в доступной форме.

**Потенциальные источники:**

- Политика компании в отношении рекламного контента,
- Центр поддержки предпринимателей компании,
- Пользовательское соглашение компании.

**F1(d). Доступ к политике использования алгоритмических систем**

Компания должна обеспечить доступ к связанным с использованием алгоритмов политикам, которые пользователи могут легко найти и понять.

*Параметры:*

1. Легко ли найти политику компании по использованию алгоритмических систем?
2. Доступны ли правила использования алгоритмических систем на основном языке (-ах), на котором (-ых) говорят пользователи в юрисдикции деятельности компании?
3. Представлены ли политики использования алгоритмических систем в понятной форме?

**Разъяснения по показателю**

[19] Предварительные показатели: Прозрачность и подотчетность стандартов таргетированной рекламы и алгоритмических систем принятия решений, *Ranking Digital Rights*, октябрь 2019 года https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-Targeted-advertising-algorithms.pdf [анг].

Применение алгоритмических систем может иметь негативные последствия в отношении фундаментальных прав человека - в частности, права на свободу самовыражения и информации, а также права на недискриминацию[20]. Помимо четкого обязательства о соблюдении и защите прав человека при разработке и внедрении подобных технологий (см. показатель G1, параметр 3), компании обязаны также опубликовать политику, в которой четко описаны условия использования алгоритмических систем в рамках их сервисов и платформ.

Помимо публикации условий предоставления услуг или пользовательских соглашений, в которых описываются запрещенные виды контента или деятельности, компании, использующие алгоритмические системы, способные причинить вред правам человека, должны публиковать четкую и доступную политику, описывающую природу и функции этих систем. В соответствии с Рекомендациями Совета Европы о воздействии алгоритмических систем на права человека [анг] 2020 года, данная политика должна быть легкодоступной, изложена простым языком и содержать опции для пользователей по управлению настройками.
Следует отметить, что в данном показателе мы рассматриваем политику, которая описывает условия применения компанией алгоритмических систем на своих платформах и сервисах.

Также важно, чтобы компании раскрывали информацию о разработке и тестировании ими алгоритмических систем, что более подробно отражено в показателе P1b.

**Потенциальные источники:**

- Политики использования алгоритмических систем,
- Руководство по развитию алгоритмических систем,
- Политика приватности или политика использования данных,
- Центр поддержки.

## F2: Уведомление об изменениях в политиках

### F2(a). Изменение условий предоставления услуг

Компания должна четко указать, что она напрямую уведомляет пользователей об изменении условий предоставления услуг до вступления этих изменений в силу.

[20] «Сценарии угроз правам человека: алгоритмы, машинное обучение и автоматизированное принятие решений», *Ranking Digital Rights*, июль 2019 года, https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-algorithms-machine-learning-automated-decision-making.pdf [анг]

*Параметры:*

1. Предоставляет ли компания четкую информацию о том, что она напрямую уведомляет пользователей обо всех изменениях в условиях предоставления услуг?
2. Предоставляет ли компания четкую информацию о том, каким именно способом она напрямую уведомляет пользователей об изменениях?
3. Предоставляет ли компания четкую информацию о сроках, в течение которых она напрямую уведомляет пользователей об изменениях до их вступления в силу?
4. Ведет ли компания публичный архив или протокол вносимых изменений?

**Разъяснения по показателю**

Изменение условий предоставления услуг по мере развития бизнеса является обычной практикой для компаний. Тем не менее, подобные изменения, включающие в себя положения о запрещенном контенте и действиях, могут существенно повлиять на свободу самовыражения и информационные права пользователей. Поэтому компании должны брать на себя обязательства по уведомлению пользователей об изменении условий и предоставлению пользователям информации, помогающей понять, что означают подобные изменения.

Данный показатель отражает, насколько четко компании раскрывают способы и временные рамки для уведомления пользователей об изменениях в условиях предоставления услуг. Предполагается, что компании обязуются напрямую уведомлять пользователей об этих изменениях до вступления изменений в силу. Порядок непосредственного уведомления может отличаться в зависимости от типа предоставляемых услуг; тем не менее, предполагается, что компании будут напрямую уведомлять своих пользователей в доступной для них форме. В отношении услуг, содержание которых включает учетные записи пользователей, подобное уведомление может состоять из сообщения электронной почты или SMS-сообщения. В отношении услуг, не требующих данных об учетной записи пользователя, прямое уведомление может включать в себя размещение хорошо читаемого объявления в точках доступа пользователей к данной услуге. Этот показатель также предусматривает подтверждение о предоставлении компанией в открытом доступе сведений о предыдущих условиях предоставления услуг, чтобы можно было понять, как они менялись с течением времени.

**Потенциальные источники:**

- Условия предоставления услуг компании

**F2(b). Изменение политики рекламного контента**

Компания должна в понятной форме указать, что она напрямую уведомляет пользователей об изменении политики рекламного контента до вступления этих изменений в силу.

*Параметры:*

1. Предоставляет ли компания четкую информацию о том, что она напрямую уведомляет пользователей об изменениях политики рекламного контента?
2. Предоставляет ли компания четкую информацию о том, каким именно способом она напрямую уведомляет пользователей об изменениях?
3. Раскрывает ли компания сроки, в течение которых она напрямую уведомляет пользователей об изменениях до того, как эти изменения вступят в силу?
4. Ведет ли компания публичный архив или протокол вносимых изменений?
5. Для мобильных экосистем: Предоставляет ли компания четкую информацию о том, что в соответствии с ее требованиями к приложениям, доступным через магазин приложений, пользователи должны быть напрямую уведомлены об изменениях в политике рекламного контента приложений компании?
6. Для экосистем персональных цифровых помощников: Предоставляет ли компания четкую информацию о том, что в соответствии с ее требованиями к навыкам помощников, доступным через ее магазин навыков, пользователи должны быть напрямую уведомлены об изменениях политики рекламного контента данных навыков?

**Разъяснения по показателю**

Изменение политики в отношении рекламного контента по мере развития бизнеса и услуг компании является обычной практикой. Тем не менее, подобные изменения, включающие в себя положения о запрещенном контенте и действиях, могут существенно повлиять на свободу самовыражения и информационные права пользователей, а также на их право на недискриминацию. Поэтому компании должны брать на себя обязательства по уведомлению пользователей об изменении условий предоставления услуг и предоставлению пользователям информации, помогающей понять, что означают подобные изменения.

Данный показатель отражает, насколько четко компании раскрывают способы и сроки уведомления пользователей об изменениях до вступления подобных изменений в

силу. Порядок непосредственного уведомления может отличаться в зависимости от типа предоставляемых услуг; тем не менее, предполагается, что компания будет напрямую уведомлять своих пользователей в доступной для них форме. В отношении услуг, содержание которых включает учетные записи пользователей, подобное уведомление может состоять из сообщения электронной почты или SMS-сообщения. В отношении услуг, не требующих данных об учетной записи пользователя, прямое уведомление может включать в себя размещение хорошо читаемого объявления в точках доступа пользователей к данной услуге. Этот показатель также предусматривает подтверждение о предоставлении компанией в открытом доступе сведений о предыдущих условиях предоставления услуг, чтобы можно было понять, как они менялись с течением времени.

**Потенциальные источники:**

- Рекламная политика, инструкции, условия предоставления услуг и т. д.;
- Рекламные объявления компании или центра поддержки бизнеса.

### F2(c). Изменение политики таргетированной рекламы

Компания должна в понятной форме указать, что она напрямую уведомляет пользователей об изменении политики таргетирования рекламы до вступления этих изменений в силу.

*Параметры:*

1. Предоставляет ли компания четкую информацию о том, что она напрямую уведомляет пользователей об изменениях политики таргетирования рекламы?
2. Предоставляет ли компания четкую информацию о том, каким именно способом она напрямую уведомляет пользователей об изменениях?
3. Раскрывает ли компания сроки, в течение которых она напрямую уведомляет пользователей об изменениях до того, как эти изменения вступят в силу?
4. Ведет ли компания публичный архив или протокол вносимых изменений?
5. Для мобильных экосистем: Предоставляет ли компания четкую информацию о том, что в соответствии с ее требованиями к приложениям, доступным через магазин приложений, пользователи должны быть напрямую уведомлены об изменениях в политике таргетирования рекламы приложений компании?

6. Для экосистем персональных цифровых помощников: Предоставляет ли компания четкую информацию о том, что в соответствии с ее требованиями к навыкам помощников, доступным через ее магазин навыков, пользователи должны быть напрямую уведомлены об изменениях политики таргетирования рекламы данных навыков?

**Разъяснения по показателю**

Изменение политики в отношении таргетированной рекламы по мере развития бизнеса и услуг компании является обычной практикой. Тем не менее, подобные изменения, включающие в себя положения о запрещенном контенте и действиях, могут существенно повлиять на свободу самовыражения и информационные права пользователей, а также на их право на недискриминацию. Поэтому компании должны брать на себя обязательства по уведомлению пользователей об изменении условий и предоставлению пользователям информации, помогающей понять, что означают подобные изменения.

Данный показатель отражает, насколько четко компании раскрывают способы и сроки уведомления пользователей об изменениях до вступления подобных изменений в силу. Порядок непосредственного уведомления может отличаться в зависимости от типа предоставляемых услуг; тем не менее, предполагается, что компании будут напрямую уведомлять своих пользователей в доступной для них форме. В отношении услуг, содержание которых включает учетные записи пользователей, подобное уведомление может состоять из сообщения электронной почты или SMS-сообщения. В отношении услуг, не требующих данных об учетной записи пользователя, прямое уведомление может включать в себя размещение хорошо читаемого объявления в точках доступа пользователей к данной услуге. Этот показатель также предусматривает подтверждение о предоставлении компанией в открытом доступе сведений о предыдущих условиях предоставления услуг, чтобы можно было понять, как они менялись с течением времени.

**Потенциальные источники:**

- Рекламная политика, инструкции, условия предоставления услуг и т. д.;
- Рекламные объявления компании или центра поддержки бизнеса.

**F2(d). Изменения политики использования алгоритмических систем**

Компания должна в понятной форме указать, что она напрямую уведомляет пользователей об изменении политики использования алгоритмических систем до вступления этих изменений в силу.

*Параметры:*

1. Предоставляет ли компания четкую информацию о том, что она напрямую уведомляет пользователей об изменениях политики использования алгоритмических систем?
2. Предоставляет ли компания четкую информацию о том, каким именно способом она напрямую уведомляет пользователей об изменениях?
3. Раскрывает ли компания сроки, в течение которых она напрямую уведомляет пользователей об изменениях до того, как эти изменения вступят в силу?
4. Ведет ли компания публичный архив или протокол вносимых изменений?

**Разъяснения по показателю**

Изменения компаниями политики использования алгоритмов могут повлиять на свободу самовыражения и информации, а также на право пользователей на недискриминацию. Поэтому компании должны брать на себя обязательства по уведомлению пользователей об изменении условий и предоставлению пользователям информации, помогающей понять, что означают подобные изменения. Этот стандарт в полной мере соответствует рекомендациям Совета Европы о воздействии алгоритмических систем на права человека [анг] 2020 года.

Данный показатель отражает, насколько четко компании раскрывают способы и временные рамки для уведомления пользователей об изменениях до вступления подобных изменений в силу. Порядок непосредственного уведомления может отличаться в зависимости от типа предоставляемых услуг; тем не менее, предполагается, что компании будут напрямую уведомлять своих пользователей в доступной для них форме. В отношении услуг, содержание которых включает учетные записи пользователей, подобное уведомление может состоять из сообщения электронной почты или SMS-сообщения. В отношении услуг, не требующих данных об учетной записи пользователя, прямое уведомление может включать в себя размещение хорошо читаемого уведомления в точках доступа пользователей к данной услуге. Этот показатель также предусматривает подтверждение о предоставлении компанией в открытом доступе сведений о предыдущих условиях предоставления услуг, чтобы можно было понять, как они менялись с течением времени.

**Потенциальные источники:**

- Политика использования алгоритмических систем,
- Инструкции по использованию алгоритмических систем,
- Политика защиты приватности или защиты данных,
- Справочный центр.

## F3: Процесс применения и соблюдения политик

### F3(a). Процесс соблюдения условий предоставления услуг

Компания должна в понятной форме указать, что она напрямую уведомляет пользователей об обстоятельствах, при которых она ограничивает контент или аккаунты пользователей.

*Параметры:*

1. Объясняет ли компания в доступной форме, какой контент или действия являются недопустимыми?
2. Объясняет ли компания в доступной форме**,** по какой причине она может ограничить аккаунт пользователя?
3. Раскрывает ли компания в доступной форме информацию о процессах, применяемых для определения контента или аккаунтов, которые нарушают правила компании?
4. Объясняет ли компания в доступной форме то, как она использует алгоритмические системы для пометки контента, нарушающего ее правила?
5. Раскрывает ли компания в доступной форме информацию о том, пользуются ли органы власти приоритетным правом отмечать контент с последующим его ограничением за нарушение правил компании?
6. Раскрывает ли компания в доступной форме информацию о том, пользуются ли физические или юридические лица приоритетным правом отмечать контент с последующим его ограничением за нарушение правил компании?
7. Объясняет ли компания в доступной форме процессы, применяемые ею, чтобы обеспечить соблюдение правил при обнаружении нарушений?

**Разъяснения по показателю**

Справедливо полагать, что компании устанавливают правила, запрещающие определенный контент или деятельность: например, токсичные высказывания или злонамеренное поведение. Однако, когда компании разрабатывают и применяют правила относительно того, что пользователи могут делать и говорить в Интернете или могут ли они вообще получить доступ к определенной услуге, то это должно делаться прозрачно и с соблюдением подотчетности.

Поэтому мы ожидаем, что компании будут в доступной форме раскрывать информацию о том, что представляют собой эти правила и как обеспечивается их соблюдение. Сюда относится также информация о том, как компании узнают о

материалах или действиях, нарушающих их условия. Например, компании могут прибегать к услугам внешних контракторов для проверки контента и/или активности пользователей. Они могут использовать механизмы отметки сообществом, которые позволяют пользователям отмечать контент и/или деятельность других пользователей для проверки компанией. Они также могут использовать алгоритмические системы для обнаружения и отметки нарушений. В этом случае компании должны объяснить, как и для каких типов контента используются эти системы. Мы ожидаем, что компании будут предоставлять четкую информацию о том, существует ли у них политика приоритетного или ускоренного рассмотрения обращений от органов власти и/или членов частных организаций или других структур, которые указывают свою организационную принадлежность при сообщении о контенте или пользователях, предположительно нарушающих правила компании. В отношении мобильных экосистем мы ожидаем раскрытия компаниями информации о типах приложений, которые они ограничивают. От экосистем персональных цифровых помощников мы ожидаем предоставления информации об ограничиваемых типах навыков и результатах поиска. При этом компании должны привести примеры, чтобы помочь пользователям понять значение правил.

**Потенциальные источники:**

- Условия предоставления услуг компаний, пользовательские соглашения;
- Политика допустимого использования компании, стандарты сообщества, правила в отношении контента, политика относительно оскорбляющего поведения или аналогичный документ, объясняющий правила, которым должны следовать пользователи;
- Поддержка компании, справочный центр, часто задаваемые вопросы.

### F3(b). Правила относительно рекламного контента и их применение

Компания должна в понятной форме указать, какими политиками она руководствуется, чтобы определять недопустимый для себя рекламный контент.

*Параметры:*

1. Объясняет ли компания в доступной форме, какие типы рекламного контента не допускаются?
2. Сообщает ли компания в доступной форме о своем требовании четкого обозначения рекламного контента?
3. Раскрывает ли компания в доступной форме процессы и технологии, использующиеся для выявления рекламного контента или аккаунтов, нарушающих правила компании?

**Разъяснения по показателю**

Компании должны четко раскрывать политику в отношении того, какие виды рекламного контента запрещены на их платформах или сервисах, а также процессы обеспечения соблюдения этих правил. В частности, этот показатель определяет, раскрывают ли компании в доступной форме типы запрещенного рекламного контента, требование четкой маркировки рекламного контента и процессы по обеспечению соблюдения этих правил.

**Потенциальные источники:**

- Портал компании для рекламодателей, рекламная политика, политика в отношении политической рекламы;
- Условия предоставления услуг компаний, пользовательские соглашения;
- Политика допустимого использования, стандарты сообщества, правила в отношении контента;
- Поддержка, справочный центр, часто задаваемые вопросы.

### F3(c). Правила таргетирования рекламы и их применение

Компания должна в доступной форме раскрывать политику, определяющую запрещенные виды таргетированной рекламы.

*Параметры:*

1. Раскрывает ли компания в доступной форме информацию о том, могут ли третьи стороны распространять таргетированный рекламный контент среди ее пользователей?
2. Объясняет ли компания в доступной форме допустимые типы параметров таргетинга?
3. Объясняет ли компания в доступной форме, что рекламодателям запрещено использовать рекламу, ориентированную на конкретного человека?
4. Объясняет ли компания в доступной форме, что сформированные алгоритмами категории рекламной аудитории до использования подвергаются проверке человеком?
5. Раскрывает ли компания в доступной форме информацию о процессах и технологиях, используемых для выявления рекламного контента или аккаунтов, нарушающих правила компании?

**Разъяснения по показателю**

Возможность для рекламодателей или других третьих сторон предоставлять пользователям контент, специально подобранный на основании их поведения в браузере, информации о местонахождении и других полученных от них данных и характеристик[21], может существенно влиять на экосистему пользователей. Таргетинг, включающий как платный, так и бесплатный контент, может усиливать социальное неравенство в офлайне и быть откровенно дискриминационным. Он также может привести к так называемым «пузырям фильтров», а также способствовать распространению сомнительного контента, в том числе направленного на введение в заблуждение или распространение ложных сведений[22].

Поэтому компании, предоставляющие рекламодателям и другим третьим сторонам возможности целевого охвата своих пользователей с помощью специально подобранной рекламы или контента, должны иметь четкие политики, описывающие правила таргетирования рекламы. Компании должны четко раскрывать, разрешают ли они третьим сторонам отображать персонализированную рекламу или контент. Они должна в доступной форме определять недопустимые параметры таргетирования, например, использование определенных категорий аудитории на основании возраста, местоположения или других характеристик пользователей. Компании также должны раскрывать свои процессы выявления нарушений правил таргетинга.

**Потенциальные источники:**

- Портал компании для рекламодателей, рекламная политика, политика в отношении политической рекламы;
- Политика допустимого использования;
- Поддержка, справочный центр, часто задаваемые вопросы для рекламодателей.

## F4: Данные о применении политики

### F4(a). Данные об ограничени контента для обеспечения выполнения условий предоставления услуг

[21] См. раздел 6.2 пилотного исследования «2020 Pilot Study and Lessons Learned», *Ranking Digital Rights*, 16 марта 2020 года, https://rankingdigitalrights.org/wp-content/uploads/2020/03/pilot-report-2020.pdf [анг]

[22] «Предварительный показатель: Прозрачность и подотчетность стандартов таргетированной рекламы и алгоритмических систем принятия решений», *Ranking Digital Rights*, октябрь 2019 года, https://rankingdigitalrights.org/wp-content/uploads/2019/10/RDR-Index-Draft-Indicators_-Targeted-advertising-algorithms.pdf [анг]

Компания должна в доступной форме и регулярно публиковать данные об объеме и сути действий, предпринятых для ограничения контента, нарушающего правила компании.

*Параметры:*

1. Публикует ли компания данные об общем количестве единиц контента, подвергшегося ограничению за нарушение правил компании?
2. Публикует ли компания данные об общем количестве единиц контента, подвергшегося ограничению за нарушение правил компании, с разбивкой по типу нарушения?
3. Публикует ли компания данные об общем количестве единиц контента, подвергшегося ограничению за нарушение правил компании, с разбивкой по типу контента (текст, изображения, видео, видеотрансляции)?
4. Публикует ли компания данные об общем количестве единиц контента, подвергшегося ограничению, с разбивкой по методу, который был использован для выявления нарушения?
5. Публикует ли компания эти данные как минимум четыре раза в год?
6. Публикует ли компания эти данные в виде структурированного файла?

**Разъяснения по показателю**

Компании могут и должны устанавливать четкие правила относительно типов контента, запрещенного на их платформах или сервисах. Этот показатель предусматривает публичное раскрытие компаниями данных о действиях, предпринимаемых ими для ограничения или иных видов цензурирования контента в связи с нарушением правил компаний. Публикация этих данных является первым важным шагом для привлечения компаний к ответственности за соблюдение собственных правил и за действия, предпринимаемые для модерации контента на их платформах и сервисах.

Компании должны публиковать данные о совокупном количестве единиц контента, который они ограничивают, удаляют или — в случае телекоммуникационных компаний — блокируют или фильтруют в результате нарушения условий предоставления услуг. Они также должны разбивать эти данные по типу нарушений и по методу, используемому для обнаружения нарушений (например, по системе отметок сообщества или по отметкам автоматизированными способами). В соответствии с «Принципами Санта-Клары» [анг] компании должны публиковать эти данные не реже четырех раз в год в виде структурированного файла данных.

**Потенциальные источники:**

- Отчет компании о прозрачности,
- Отчет компании о соблюдении стандартов сообщества, отчет о соблюдении правил сообщества и т. д.

### F4(b). Данные об ограничениях аккаунтов с целью обеспечения соблюдения условий предоставления услуг

Компания должна регулярно в доступной форме публиковать данные об объеме и сути действий, предпринятых для ограничения аккаунтов, нарушающих правила компании.

*Параметры:*

1. Публикует ли компания данные об общем количестве аккаунтов, подвергшихся ограничению за нарушение правил компании?
2. Публикует ли компания данные об общем количестве единиц аккаунтов, подвергшихся ограничению за нарушение правил компании, с разбивкой по типу нарушения?
3. Публикует ли компания данные об общем количестве аккаунтов, подвергшихся ограничению за нарушение правил компании, с разбивкой по методу, использованному для выявления нарушения?
4. Публикует ли компания эти данные как минимум четыре раза в год?
5. Публикует ли компания эти данные в виде структурированного файла?

**Разъяснения по показателю**

Компании могут и должны устанавливать виды контента или деятельности, не допустимых на их платформах или сервисах. Этот показатель предполагает, что компании будут публично раскрывать данные о действиях, которые они предпринимают для обеспечения соблюдения правил компании. Публикация этих данных является первым важным шагом для привлечения компаний к ответственности за соблюдение собственных правил и за действия, которые они предпринимают для модерации контента на своих платформах и сервисах.

Компании должны публиковать данные о количестве аккаунтов, подвергнутых ограничению в результате нарушения условий предоставления услуг. Они также должны разбивать эти данные по типу нарушений и по методу, используемому для

обнаружения нарушений (например, по системе отметок сообщества или по отметкам автоматизированными способами). В соответствии с «Принципами Санта-Клары» [анг] компании должны публиковать эти данные не реже четырех раз в год в виде структурированного файла данных.

**Потенциальные источники:**

- Отчет компании о прозрачности.

**F4(c). Данные о применении политики относительно рекламного контента и таргетинга**

Компания должна регулярно в доступной форме публиковать данные об объеме и сути действий, предпринимаемых ею для ограничения рекламного контента, опубликованного с нарушением рекламной политики компании и политики в отношении таргетированной рекламы.

*Параметры:*

1. Раскрывает ли компания общее количество рекламных сообщений, подвергнутых ограничению в целях обеспечения соблюдения политики в отношении рекламного контента?
2. Раскрывает ли компания общее количество подвергнутых ограничению рекламных сообщений с разбивкой по типу нарушения правил в отношении рекламного контента?
3. Раскрывает ли компания общее количество подвергнутых ограничению рекламных сообщений в целях обеспечения соблюдения политики таргетинга рекламы?
4. Раскрывает ли компания общее количество подвергнутых ограничению рекламных сообщений с разбивкой по типу нарушения правил в отношении таргетирования рекламы?
5. Публикует ли компания эти данные как минимум один раз в год?
6. Публикует ли компания эти данные в виде структурированного файла?

**Разъяснения по показателю**

Показатели F3c и F3d отражают требование к компаниям публиковать в доступной форме правила о запрещенных типах рекламного контента и таргетированной рекламы, а также описания процессов обеспечения соблюдения этих правил. Показатель F4c отражает требование к компаниям публиковать доказательства того,

что они обеспечивают соблюдение этих правил. Компании должны публиковать данные об общем количестве рекламных сообщений, удаленных в результате нарушения политики в отношении рекламного контента, с разбивкой по типу нарушения. Компании также должны предоставить доказательства того, что они обеспечивают соблюдение политики таргетирования рекламы, публикуя данные о количестве объявлений, удаленных за нарушение правил таргетинга, и о том, какое правило было нарушено. Компании также должны публиковать эти данные не реже одного раза в год и в виде структурированного файла данных.

**Потенциальные источники:**

- Отчет компании о прозрачности.

## F5: Процесс реагирования на требования третьих сторон ограничить контент или аккаунты

### F5(a). Процесс реагирования на требования властей

Компания должна в доступной форме предоставлять информацию о процессе реагирования на требования властей (в том числе судебные решения) об удалении, фильтрации или ограничении контента или аккаунтов.

*Параметры:*

1. Предоставляет ли компания в доступной форме информацию о процессе реагирования на внесудебные требования властей?
2. Предоставляет ли компания в доступной форме информацию о процессе реагирования на судебные решения?
3. Предоставляет ли компания в доступной форме информацию о процессе реагирования на требования властей иностранных государств?
4. Разъясняет ли компания в доступной форме правовые основания, на которых она может выполнить требование властей?
5. Разъясняет ли компания в доступной форме, что она проявляет должную осмотрительность, перед тем как отреагировать на требования властей?
6. Обязуется ли компания противостоять неправомерным или чрезмерно широким требованиям властей?
7. Предоставляет ли компания изложенные в доступной форме руководства или примеры реализации своего процесса реагирования на требования властей?

**Разъяснения по показателю**

Компании часто получают от правительств требования удалить, отфильтровать или ограничить доступ к контенту и учетным записям. Такие требования могут исходить от правоохранительных органов и судов (местных или зарубежных), а также от других государственных органов. Мы ожидаем от компаний публичного раскрытия информации по процессам реагирования на подобные требования. Компании должны предоставить юридические основания для выполнения требований органов власти, а также заявить о четком намерении противостоять необоснованным требованиям.

Наше определение требований со стороны властей включает в себя и «внесудебный» порядок вынесения требований: например, приказы правоохранительных органов, а также гражданские иски от частных лиц. Требования на блокировку, поступающие в соответствие с организованными процессами, например, согласно Закону США об авторском праве в цифровую эпоху или европейском праве на забвение, определяются как поступающие в частном порядке и оцениваются в показателе F5b ниже.

**Потенциальные источники:**

- Отчет компании о прозрачности,
- Руководство компании по общению с органами правопорядка,
- Ежегодные отчеты компании.

### F5(b). Процесс реагирования на частные запросы об ограничении контента или аккаунтов

Компания должна в доступной форме предоставлять информацию о процессе реагирования на поступающие в частном порядке запросы об удалении, фильтрации или ограничении контента или аккаунтов.

*Параметры:*

1. Предоставляет ли компания в доступной форме информацию о процессах реагирования на поступившие в частном порядке запросы об удалении, фильтрации или ограничения контента или аккаунтов?
2. Разъясняет ли компания в доступной форме основания, на которых она может отреагировать на запросы, поступившие в частном порядке?

3. Разъясняет ли компания в доступной форме, что она проявляет должную осмотрительность, перед тем как отреагировать на запросы, поступившие в частном порядке?
4. Обязуется ли компания противостоять неправомерным или чрезмерно широким запросам, поступившим в частном порядке?
5. Предоставляет ли компания изложенные в доступной форме руководства или примеры реализации процесса реагирования на запросы, поступившие в частном порядке?

**Разъяснения по показателю**

Помимо требований правительств и других органов власти, компании могут получать частные запросы на удаление или ограничение доступа к контенту и аккаунтам. Такие запросы могут поступать в рамках установленных законом формальных процессов (например, в соответствии с американским Законом об авторском праве в цифровую эпоху или европейским правом на забвение) или в рамках саморегулируемых процессов (например, в результате соглашений компаний о блокировании определенных типов материалов или изображений в соответствии с Кодексом практики ЕС по дезинформации). В данном показателе не рассматриваются частные запросы, поступающие через какой-либо суд или в рамках судебного процесса, так как они рассматриваются в рамках запросов, поступающих от государственных органов (показатель F5a).

Данный показатель оценивает, раскрывает ли компания четкую информацию о том, как она реагирует на поступающие частным образом запросы об удалении, фильтрации или ограничении контента или учетных записей (параметр 1). Компания должна раскрыть основания для удовлетворения таких запросов (параметр 2), а также сообщить, проявляет ли она должную осмотрительность перед принятием решений о том, как реагировать на подобные запросы (параметр 3). Мы также ожидаем, что компании обязуются противодействовать чрезмерно широким частным запросам на удаление контента или учетных записей (параметр 4) и публиковать примеры, явно иллюстрирующие, как компании обрабатывают такие запросы (параметр 5).

**Потенциальные источники:**

- Отчет компании о прозрачности,
- Центр поддержки компании,
- Публикации в блоге компании,
- Политика компании в отношении авторских прав или интеллектуальной собственности.

## F6. Данные о требованиях властей ограничить доступ к контенту или аккаунтам

Компания должна регулярно публиковать данные о требованиях властей (включая судебные постановления) об удалении, фильтрации или ограничении контента и аккаунтов.

*Параметры:*

1. Предоставляет ли компания данные о количестве полученных подобных требований с разбивкой по странам?
2. Предоставляет ли компания данные о количестве затронутых таким образом аккаунтов?
3. Указывает ли компания данные о том, какое количество единиц контента или URL-адресов было затронуто?
4. Приводит ли компания перечень категорий тем, связанных с полученными требованиями?
5. Указывает ли компания общее количество требований, исходящих от различных официальных органов?
6. Указывает ли компания количество требований на ограничение контента или аккаунтов, поступивших от официальных лиц по неформальным каналам?
7. Указывает ли компания количество выполненных ею требований?
8. Оглашает ли компания информацию об исходных требованиях или информирует ли о предоставлении соответствующих копий в сторонний публичный архив?
9. Публикует ли компания эти данные как минимум один раз в год?
10. Можно ли экспортировать эти данные в виде структурированного файла?

### Разъяснения по показателю

Компании достаточно часто получают от органов власти запросы на удаление, фильтрацию или ограничение контента или аккаунтов. Предполагается, что компании будут на постоянной основе публиковать сведения о количестве и типах получаемых ими правительственных запросов, а также о количестве удовлетворенных запросов. Подобные требования могут быть получены компаниями как в рамках официального процесса (например, по решению суда), так и по неформальным каналам (например, через систему отметок, предназначенную для того, чтобы отдельные лица могли информировать о контенте, нарушающем условия предоставления услуг). Компании

должны быть максимально прозрачными в отношении содержания подобных запросов. Если компания осведомлена о поступлении запроса от судебного или иного государственного органа, она должна указать это в своей отчетности по поступающим правительственным запросам. Раскрытие подобных данных способствует лучшему пониманию общественностью взаимоотношений между компаниями и правительствами в области контроля сетевого контента, а также способствует повышению степени ответственности компаний и властей в отношении соблюдения и защиты права на свободу самовыражения.

В ряде случаев законодательство может препятствовать разглашению компанией информации, упомянутой в настоящем показателе. Например, предполагается, что компании будут публиковать точные данные, а не диапазоны значений. Однако следует признать, что законодательство в некоторых случаях препятствует подобным действиям со стороны компаний, поэтому в каждом отдельном случае подобные ситуации могут быть задокументированы исследователями. Тем не менее, в случае несоответствия другим перечисленным выше стандартам компания потеряет значительное количество пунктов. Иногда законодательство препятствует компаниям в их стремлении внедрять передовые практики, но мы призываем компании выступать за принятие законов, позволяющих им в полной мере соблюдать права пользователей на свободу самовыражения и неприкосновенность частной жизни.

**Потенциальные источники:**

- Отчет о прозрачности компании.

### F7. Данные о частных запросах на ограничение контента или аккаунтов

Компания должна регулярно публиковать данные о частных запросах на удаление, фильтрацию или ограничение контента и аккаунтов.

*Параметры:*

1. Предоставляет ли компания данные о количестве полученных частных запросов на ограничение контента и аккаунтов?
2. Предоставляет ли компания данные о количестве затронутых таким образом аккаунтов?
3. Указывает ли компания данные о том, какое количество единиц контента или URL-адресов было таким образом затронуто?
4. Приводит ли компания данные о причинах удаления контента в связи с полученными требованиями?

5. Предоставляет ли компания в доступной форме информацию о полученных частных запросах?
6. Указывает ли компания количество выполненных ею требований?
7. Оглашает ли компания информацию об исходных требованиях или информирует ли о предоставлении соответствующих копий в сторонний публичный архив?
8. Публикует ли компания эти данные как минимум один раз в год?
9. Можно ли экспортировать эти данные в виде структурированного файла?
10. Предоставляет ли компания в доступной форме информацию о том, что представляемая ею отчетность содержит перечень всех типов частных запросов?

**Разъяснения по показателю**

Компании достаточно часто получают частные запросы на удаление, фильтрацию или ограничение контента или аккаунтов. Эти запросы могут быть поданы на основании Закона США об авторском праве в цифровую эпоху или европейского права на забвение, а также в рамках механизмов саморегулирования (например, соглашений между компаниями о блокировке определенных типов изображений). Предполагается, что компании на постоянной основе публикуют сведения о количестве и типах получаемых ими частных запросов, а также о количестве удовлетворенных запросов подобного типа.

**Потенциальные источники:**

- Отчет о прозрачности компании.

### F8. Оповещение пользователей об ограничении контента и аккаунтов

Компания должна указать в доступной форме то, что она извещает пользователей в случае ограничения контента или аккаунтов.

*Параметры:*

1. Для компаний, размещающих на своих платформах пользовательский контент. Предоставляет ли компания в доступной форме информацию о том, что пользователи, чей контент подвергнут ограничениям, получают об этом уведомление?
2. Сообщает ли компания в доступной форме, что она уведомляет пользователей при попытке получить доступ к ограниченному контенту?

3. Указывает ли компания в своем уведомлении причину ограничения контента (юридические или иные основания) в доступной форме?
4. Сообщает ли компания в доступной форме, что она извещает пользователей в случае ограничения их аккаунта?

**Разъяснения по показателю**

Если показатель F3 отражает уровень раскрытия компанией информации об ограничениях публикаций и действий пользователей в рамках отдельного сервиса, то показатель F8 направлен на выявление того, достаточно ли четко компания предоставляет информацию об уведомлении пользователей в случае принятия ограничительных мер (будь то в связи с выполнением условий предоставления услуг или в результате запросов третьих сторон).

Принятие компанией решения об ограничении или о прекращении доступа к контенту или аккаунтам может оказать существенное влияние на свободу самовыражения пользователей и их права на доступ к информации. По этой причине от компании ожидается обязательное информирование пользователей об удалении контента, ограничении доступа к аккаунту или других ограничениях доступа к услугам и сервисам. Если компания удаляет опубликованный пользователем контент, предполагается, что пользователь будет проинформирован о таком решении. В случае попыток доступа к ограниченному компанией контенту другим пользователем предполагается, что компания уведомляет пользователя об ограничении доступа к этому контенту. Также мы ожидаем, что компании называют причины принятия подобных решений. Такое информирование является обязательной составляющей при разъяснении компаниями своей практики по ограничению контента и доступа к нему.

**Потенциальные источники:**

- Условия предоставления услуг компании, политика допустимого использования;
- Стандарты сообщества компании;
- Страница поддержки, справочный центр или FAQ;
- Рекомендации компании для разработчиков;
- Политика компании в области прав человека.

## F9. Управление сетями (телекоммуникационные компании)

Компания должна предоставлять в доступной форме информацию о том, что она не приоритезирует, не блокирует и не замедляет определенные типы трафика,

приложений, протоколов или контента по каким-либо причинам, не связанным с обеспечением качества обслуживания и надежной работы сети.

*Параметры:*

1. Заявляет ли компания в доступной форме об обязательствах следования политике отказа от приоритезации, блокировки или задержки определенных типов трафика, приложений, протоколов или контента по причинам, не связанным с обеспечением качества обслуживания и надежности работы сети?
2. Прибегает ли компания к практикам программ нулевого рейтинга, которые определяют приоритетность сетевого трафика по причинам, не связанным с обеспечением качества обслуживания и надежности работы сети?
3. Если компания применяет практику приоритезации сетевого трафика по причинам, не связанным с обеспечением качества обслуживания и надежности работы сети, разъясняет ли она четко свои мотивы?

**Разъяснения по показателю**

Данный показатель позволяет оценить, насколько отчетливо телекоммуникационные компании раскрывают информацию о применении ими практических мер регулирования потока контента через свои сети, например, о замедлении или изменении структуры трафика. Предполагается, что компании возьмут на себя публичные обязательства по недопущению приоритизации или урезанию контента. В ряде случаев компании могут применять законные методы распределения трафика, чтобы обеспечить его поток по своим сетям. В таких случаях предполагается, что компания сделает официальное заявление с разъяснением мотивов соответствующих действий. Однако компании могут использовать платные методы приоритизации или программы нулевого рейтинга, не являющиеся легитимными методами управления сетью. Например, компания может разместить на своем сайте заявление о приверженности принципам сетевого нейтралитета, но при этом предлагать услуги нулевого рейтинга.

**Потенциальные источники:**

- Политика компании по управлению сетями или трафиком,
- Годовые отчеты компании.

### F10. Отключение сети (телекоммуникационные компании)

Компании должны в доступной форме описать обстоятельства, при которых возможно отключение или ограничение доступа к сети, определенным протоколам, службам или приложениям в сети.

*Параметры:*

1. Разъясняет ли компания в доступной форме причину (причины) для прекращения обслуживания определенной зоны или группы пользователей?
2. Разъясняет ли компания в доступной форме причину (причины) для ограничения доступа к определенным приложениям или протоколам (например, VoIP, обмен сообщениями) в определенной зоне или для определенной группы пользователей?
3. Раскрывает ли компания в доступной форме план действий в случае требований властей отключить сеть или ограничить доступ к услугам?
4. Заявляет ли компания о своей готовности противостоять требованиям властей по отключению сети или ограничению доступа к услугам?
5. Сообщает ли компания в доступной форме о прямом уведомлении пользователей в случае отключения сети или ограничения доступа к услугам?
6. Раскрывает ли компания в доступной форме информацию о количестве получаемых ею запросов на отключение сети?
7. Раскрывает ли компания в доступной форме информацию о том, какой именно орган власти выдвигает такие требования?
8. Раскрывает ли компания в доступной форме информацию о числе выполненных подобных требований государственных органов?

**Разъяснения по показателю**

Отключение сетей представляет все большую угрозу соблюдению прав человека. Совет по правам человека ООН осуждает действия по отключению сетей как нарушающие международные законы о правах человека и требует от властей не прибегать к подобным действиям[23]. Однако государственные органы все чаще стали предписывать телекоммуникационным компаниям отключение сетей[24], что, в свою очередь, вынуждает компании предпринимать действия, противоречащие принципам соблюдения прав человека. В связи с этим предполагается, что компании будут

[23] «Поощрение, защита и поощрение прав человека в Интернете», Совет ООН по правам человека (32 сессия), 27 июня 2016 года, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement [анг]
[24] #KeepItOn, *Access Now,* https://www.accessnow.org/keepiton/ [анг], последняя дата доступа: 2 апреля 2020 года.

полностью разглашать все обстоятельства, при которых они могут предпринять такие действия, а также сообщать о полученных ими требованиях о принятии таких мер и раскрывать информацию об обязательствах по противодействию или минимизации последствий подобных требований властей.

**Потенциальные источники:**

- Условия предоставления услуг компании,
- Отчет компании о прозрачности,
- Руководство компании по соблюдению законодательства,
- Политика компании по правам человека.

### F11. Политика идентификации пользователей

Компания не должна обязывать пользователей подтверждать свою личность с помощью документов удостоверения личности, выданных государственным органом, или иных видов идентификационных данных, которые могут быть использованы для идентификации личности оффлайн.

1. Требует ли компания подтверждения личности пользователей с помощью удостоверяющего личность документа, выданного государственным органом, или посредством другого вида идентификационных данных, которые могут быть использованы для идентификации личности оффлайн?

**Разъяснения по показателю**

Компания не должна обязывать пользователей подтверждать свою личность с помощью удостоверяющего личность документа, выданного государственным органом, или посредством иных видов идентификационных документов, которые могут быть использованы для установления личности пользователей оффлайн.

Возможность анонимного общения необходима для обеспечения свободы выражения мнений как в сети, так и за ее пределами. Использование подлинного имени в Интернете или требование от пользователей предоставить компании идентифицирующую информацию позволяет установить связь между деятельностью в Интернете и конкретным человеком. Это таит в себе связанные с правами человека риски для тех, кто, например, высказывает мнение, не совпадающее с мнением властей, или участвует в активистской деятельности, запрещенной государственной властью. Кроме того, это несет в себе риски в отношении людей, подвергающихся преследованиям за религиозные убеждения или сексуальную ориентацию.

В связи с этим предполагается, что компании будут раскрывать информацию о том, просят ли они своих пользователей о подтверждении своей личности с помощью идентифицирующих документов, выданных государственными органами, или посредством других видов идентификации, которые могут быть связаны с личными данными пользователей оффлайн. К прочим средствам идентификации относятся кредитные карты и зарегистрированные номера телефонов. Следует отметить, что для получения доступа к платным функциям различных видов продуктов и услуг пользователю может потребоваться предоставить сведения, связанные с его личностью оффлайн. Тем не менее, пользователи должны иметь возможность получать доступ к бесплатным услугам без необходимости предоставлять информацию, которая может быть привязана к их персональным данным оффлайн. В ряде случаев телефонные номера могут быть связаны с идентичностью пользователей оффлайн. Например, в правовом контексте, при котором пользователи предоплаченных услуг обязаны регистрироваться с указанием своих идентификационных данных. Даже если предоставление номера телефона является необходимым условием предоставления услуги (например, в случае приложений для обмена мгновенными сообщениями), компании могут получить максимальную оценку по данному показателю при условии, что они не требуют от пользователей предоставления персональных данных или предоставления документов, подтверждающих личность.

Сервисы, которые запрашивают у пользователей номер телефона для целей, не являющихся необходимыми для предоставления услуги, не получают никакой оценки. Например, некоторые сервисы могут запрашивать номер телефона в целях двухфакторной аутентификации; однако это должно быть опционально, и пользователям должны быть предоставлены другие варианты двухфакторной аутентификации.

Данный показатель применим к компаниям-цифровым платформам и предоплаченным услугам мобильных систем (для телекоммуникационных компаний).

**Потенциальные источники:**

- Условия предоставления услуг или эквивалентная документация,
- Справочный центр компании,
- Страница регистрации на сервисе компании.

### F12. Алгоритмическое курирование контента, рекомендации и/или системы ранжирования

Компании должны в доступной форме объяснять, каким образом пользовательский контент подвергается курированию, ранжированию и/или рекомендации.

*Параметры:*

1. Предоставляет ли компания в доступной форме информацию о применении ею алгоритмических систем для курирования, рекомендации и/или ранжирования контента, доступного пользователям на ее платформе?
2. Объясняет ли компания в доступной форме, каким образом она использует алгоритмические системы для курирования, рекомендации и/или ранжирования контента, а также, какие переменные влияют на эти системы?
3. Объясняет ли компания в доступной форме, какие возможности есть у пользователей, чтобы контролировать переменные, учитываемые алгоритмической системой курирования, рекомендации и/или ранжирования контента?
4. Раскрывает ли компания в доступной форме информацию об использовании алгоритмических систем для автоматического курирования, рекомендации и/или ранжирования контента по умолчанию?
5. Объясняет ли компания в доступной форме, что у пользователей есть возможность согласиться с автоматическим курированием, рекомендацией и/или ранжированием контента?

**Разъяснения по показателю**

Алгоритмические системы курирования, рекомендации и ранжирования контента играют важнейшую роль в формировании того, к каким типам контента и информации пользователи могут получать доступ. Кроме того, системы, оптимизированные для вовлечения пользователей, могут иметь эффект приоритетизирования спорного и подстрекательского контента, включая контент, который не защищен международным правом в области прав человека. Со временем зависимость от алгоритмических систем курирования и рекомендаций, оптимизированных для вовлечения пользователей, может изменить новостные и информационные экосистемы целых стран или сообществ. Этими системами можно манипулировать для распространения дезинформации и иного искажения информационной экосистемы, что, в свою очередь, может способствовать нарушениям прав человека.

Поэтому компании должны быть прозрачными в отношении использования ими автоматизированных систем курирования, рекомендации и ранжирования, включая раскрытие переменных, влияющих на такие системы. Компании должны публиковать информацию о том, используют ли они алгоритмические системы для курирования, рекомендации и ранжирования контента. Они должны раскрывать информацию о том, как работают эти системы, какие возможности есть у пользователей, чтобы

контролировать использование их информации этими системами, включены ли такие системы по умолчанию или пользователи могут по желанию включить автоматическое курирование их контента алгоритмической системой.

**Потенциальные источники:**

- Политика компании в области прав человека;
- Политика компании в области использования искусственного интеллекта, в том числе принципы использования искусственного интеллекта, правовые рамки и руководства по применению;
- Страницы справочника с перечислением того, как алгоритмы влияют на настройки новостной ленты, настройки домашней страницы, результаты поиска, рекомендации, интересы пользователя и темы.

### F13. Автоматизированные программные агенты («боты»)

Компании должны в доступной форме разъяснять свою политику использования автоматизированных программных агентов («ботов») на своих платформах, в продуктах и услугах, а также то, каким образом обеспечивается соблюдение этой политики.

*Параметры:*

Разъясняет ли компания в доступной форме правила, регулирующие использование ботов на ее платформе?

1. Указывает ли компания в доступной форме, что пользователи должны ясно помечать любой контент и аккаунты, созданные, распространяемые или управляемые с помощью бота?
2. Разъясняет ли компания в доступной форме процесс обеспечения исполнения политики в отношении ботов?
3. Раскрывает ли компания в доступной форме данные об объеме и характере пользовательского контента и аккаунтов, подвергнутых ограничениям за нарушение политики компании в отношении ботов?

**Разъяснения по показателю**

Платформы социальных сетей часто позволяют пользователям создавать автоматизированные программные агенты, или «боты», которые автоматизируют различные действия, выполняемые учетной записью пользователя — такие, как публикация или продвижение контента (например, с помощью ретвитов). Существует

множество безобидных и даже положительных применений ботов: например, художники используют ботов Twitter для пародий[25]. Однако есть и более проблематичные виды их использования, которые многие компании запрещают или не поощряют. Например, когда политические партии или их доверенные лица используют бот-сети для продвижения определенных сообщений или для искусственного раздувания аудитории кандидата с целью манипулирования общественным дискурсом и результатами выборов. На некоторых платформах социальных сетей боты или скоординированные сети ботов («ботнеты») могут использоваться для преследования пользователей («бригадирство»), искусственного усиления определенного контента (массовые ретвиты и т. д.) и других искажений общественного дискурса на платформе. Некоторые эксперты призывают компании требовать от пользователей, использующих ботов, явного обозначения их как ботов, чтобы помочь обнаружить такие искажения[26]. Поэтому компании, разрешающие использование ботов, должны иметь четкую политику, регулирующую использование ботов на своих платформах. Они должны сообщать, требуют ли они, чтобы контент и аккаунты, которые создаются, распространяются или управляются с помощью бота, были помечены как таковые. Они также должны разъяснять процесс обеспечения соблюдения политики использования ботов, в том числе путем публикации данных об объеме и характере контента и аккаунтов, которые были ограничены за нарушение этих правил.

**Потенциальные источники:**

- Политики платформы для разработчиков,
- Правила использования автоматизации или ботов,
- Отчеты о прозрачности.

[25] *Thinkpiece Bot*, Twitter, https://twitter.com/thinkpiecebot, последняя дата доступа: 2 апреля 2020 года.

[26] Engler, A.: The case for AI transparency requirements. Brookings Institution, 22 января 2020 года https://www.brookings.edu/research/the-case-for-ai-transparency-requirements/, последняя дата доступа: 2 апреля 2020 года.

# Приватность

Показатели этой категории отражают стремление компаний доступно, на примерах своей политики и ее практического воплощения разъяснять свою приверженность праву пользователей на приватность в соответствии со Всеобщей декларацией прав человека[27], с Международным пактом о гражданских и политических правах[28] и другими международными инструментами соблюдения правам человека. Открытая политика и практики компаний демонстрируют, как они стараются не способствовать действиям, которые могут нарушить неприкосновенность частной жизни пользователей, за исключением случаев, когда такие действия являются законными, соразмерными и преследуют оправданную цель. Они также демонстрируют твердую приверженность защите и охране цифровой безопасности пользователей. Компании, демонстрирующие высокие результаты по этим показателям, демонстрируют твердую приверженность прозрачности не только в том, как они реагируют на требования правительства и других лиц, но и в том, как они определяют, передают и обеспечивают соблюдение собственных правил и отраслевых практик, влияющих на приватность пользователей.

### P1: Доступ к политике, затрагивающей приватность пользователей

#### P1(a). Доступ к политике приватности

Политика приватности компании должна быть опубликована в таком виде, чтобы пользователям было легко ее найти и легко понять.

*Параметры:*

1. Легко ли найти политику приватности компании?
2. Опубликована ли политика приватности компании на основном языке (-ах) общения пользователей в стране ее национальной юрисдикции?
3. Изложена ли эта политика в легко доступном для понимания виде?
4. Для мобильных экосистем: Раскрывает ли компания тот факт, что в соответствии с требованиями к приложениям, доступным через ее магазин

[27] Всеобщая декларация прав человека, ООН, https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml

[28] Международный пакт о гражданских и политических правах, Управление Верховного комиссара ООН по правам человека, https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml

приложений, пользователям должен быть предоставлен доступ к политике приватности?

5. Для экосистем персональных цифровых помощников: Предоставляет ли компания информацию о том, что в соответствии с требованиями к навыкам помощников, доступным через ее магазин навыков, пользователям должен быть предоставлен доступ к политике приватности?

**Разъяснения по показателю**

Политика приватности отражает, как компании собирают, управляют, используют и защищают информацию о пользователях, а также информацию, предоставленную самими пользователями. Учитывая это, компании должны убедиться, что их пользователи без труда могут сами найти описание этой политики и понять, что она означает. Данный показатель предполагает, что компании будут публиковать политику приватности, которую легко найти, легко понять и которая доступна на основных языках общения на домашнем рынке компании. Если компания предлагает несколько продуктов и услуг, должно быть ясно, к каким продуктам и услугам относится конкретная политика приватности.

Если документ легко найти, это значит, что он доступен прямо на домашней странице компании или сайте сервиса. Он должен быть расположен в нескольких кликах от главной страницы или быть иным образом доступен в логичном месте, где пользователи, скорее всего, найдут его. Положения политики также должны быть доступны на основном языке (основных языках) национального рынка. Кроме того, мы ожидаем, что компании предпримут шаги, чтобы помочь пользователям понять информацию, представленную в их правилах. Это можно сделать, например, при помощи краткого изложения, советов или рекомендаций, объясняющих значение терминов, а также при помощи заголовков разделов, удобочитаемого шрифта и других графических средств, повышающих доступность документа.

**Потенциальные источники:**

- Политика приватности,
- Политика использования данных.

### P1(b). Доступ к политике разработки алгоритмических систем

У компании должна быть легко доступная и понятная политика разработки алгоритмических систем.

*Параметры:*

1. Легко ли найти политику разработки алгоритмических систем компании?
2. Опубликована ли политика разработки алгоритмических систем компании на основном языке (-ах) общения ее пользователей?
3. Понятно ли изложены положения политики разработки алгоритмических систем?

**Разъяснения по показателю**

Разработка и тестирование алгоритмических систем может представлять значительный риск для приватности пользователей, особенно когда компании используют собранную информацию о пользователях для разработки, обучения и тестирования этих систем без информированного согласия субъекта данных[29]. Компании должны четко раскрывать политику, описывающую разработку и тестирование алгоритмических систем, в доступной, легко читаемой и понятной пользователям форме, чтобы пользователи могли принимать информированные решения об использовании продуктов и услуг компании.

**Потенциальные источники:**

- Политика использования алгоритмических систем,
- Руководство по разработке алгоритмических систем,
- Политика приватности или использования данных.

## P2: Уведомление об изменениях

### P2(a). Изменения политики приватности

Компания должна в доступной форме сообщать, что она прямо оповещает пользователей об изменениях политики приватности до их вступления в силу.

[29] Зубофф Ш., The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Нью-Йорг, США: PublicAffairs, 2019; Натали Маришаль, Targeted Advertising Is Ruining the Internet and Breaking the World, https://www.vice.com/en_us/article/xwjden/targeted-advertising-is-ruining-the-internet-and-breaking-the-world [анг], *Vice Motherboard,* 16 ноября 2018; «Сценарии угроз правам человека: алгоритмы, машинное обучение и автоматизированное принятие решений», *Ranking Digital Rights*, июль 2019 года, https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-Risk-Scenarios_-algorithms-machine-learning-automated-decision-making.pdf [анг]

*Параметры:*

1. Сообщает ли компания в доступной форме, что она прямо уведомляет пользователей об изменениях политики приватности?
2. Разъясняет ли компания в доступной форме, как именно она прямо уведомляет пользователей об изменениях?
3. Публикует ли компания в доступной форме сроки, в течение которых она прямо оповещает пользователей об изменениях политики приватности до их вступления в силу?
4. Ведет ли компания публичный архив или протокол вносимых изменений
5. Для мобильных экосистем: Сообщает ли компания в доступной форме о том, что приложения, доступные через ее магазин приложений, должны уведомлять пользователей об изменении политики приватности?
6. Для экосистем персональных цифровых помощников: Сообщает ли компания в доступной форме о том, что навыки, доступные через ее магазин навыков, должны уведомлять пользователей об изменении политики приватности?

**Разъяснения по показателю**

По мере развития бизнеса компании часто меняют свою политику приватности. Однако эти изменения могут повлиять на права пользователя на приватность, изменив то, какую информацию о пользователе компании могут собирать, передавать и хранить. Поэтому мы ожидаем, что компании будут уведомлять пользователей при изменении политику и предоставлять им информацию, которая поможет понять, что означают эти изменения.

Данный показатель оценивает, насколько ясно компании раскрывают свои методы и сроки уведомления пользователей об изменениях в политике приватности. Мы ожидаем, что компании обязуются напрямую уведомлять пользователей до вступления изменений в силу. Метод прямого уведомления может отличаться в зависимости от типа услуги. Для услуг, требующих наличия учетной записи пользователя, прямое уведомление может включать отправку электронного письма или SMS. Для услуг, не требующих учетной записи пользователя, прямое уведомление должно включать размещение заметного уведомления на главной веб-странице или платформе, через которую пользователи получают доступ к услуге. Этот показатель также требует подтверждения того, что компания предоставляет общедоступные записи о предыдущих политиках, чтобы можно было понять, как политика компании менялась с течением времени.

**Потенциальные источники:**

- Политика приватности,
- Политика использования данных.

**P2(b). Изменения политики разработки алгоритмических систем**

Компания должна в доступной форме сообщать о том, что она напрямую уведомляет пользователей об изменениях политики разработки алгоритмических систем до вступления этих изменений в силу.

*Параметры:*

1. Сообщает ли компания в доступной форме о том, что она напрямую уведомляет пользователей об изменениях политики разработки алгоритмических систем?
2. Разъясняет ли компания в доступной форме, как именно она напрямую уведомляет пользователей об изменениях?
3. Публикует ли компания в доступной форме график, по которому она прямо оповещает пользователей об изменениях ее политики до их вступления в силу?
4. Ведет ли компания публичный архив или протокол вносимых изменений?

**Разъяснения по показателю**

По мере развития бизнеса компании могут менять политику разработки алгоритмических систем. Однако эти изменения могут оказать значительное влияние на право пользователей на неприкосновенность частной жизни. Поэтому, в соответствии с Рекомендацией Совета Европы о воздействии алгоритмических систем на права человека (2020), мы ожидаем, что компании будут уведомлять пользователей об изменениях в этой политике и предоставлять пользователям информацию, которая поможет им понять значение этих изменений.

Данный показатель оценивает, насколько четко компании раскрывают методы и сроки уведомления пользователей об изменениях политики приватности. Мы ожидаем, что компании обязуются напрямую уведомлять пользователей до вступления изменений в силу. Метод прямого уведомления может отличаться в зависимости от типа услуги. Для услуг, требующих наличия учетной записи пользователя, прямое уведомление может включать отправку электронного письма или SMS. Для услуг, не требующих учетной записи пользователя, прямое уведомление должно включать размещение заметного уведомления на главной веб-странице или платформе, через которую пользователи получают доступ к услуге. Этот показатель оценивает также, может ли компания подтвердить, что предоставляет общедоступные записи о предыдущих

политиках, чтобы можно было понять, как политика компании менялась с течением времени.

**Потенциальные источники:**

- Политика использования алгоритмических систем,
- Политика приватности или политика использования данных.

## P3: Сбор и обработка пользовательских данных

### P3(a). Сбор пользовательских данных

Компания должна в доступной форме разъяснять, какие пользовательские данные и как она собирает.

*Параметры:*

1. Раскрывает ли компания в доступной форме, какие пользовательские данные и как она собирает?
2. Раскрывает ли компания в доступной форме, как она собирает пользовательские данные по каждому типу этих данных?
3. Разъясняет ли компания в доступной форме, что она ограничивает сбор пользовательских данных исключительно тем, что непосредственно необходимо для предоставления ее услуг?
4. Для мобильных экосистем: Разъясняет ли компания в доступной форме, что она проверяет наличие в политике приватности приложений сторонних разработчиков, доступных в ее магазине приложений, информацию о сборе пользовательских данных этими приложениями?
5. Для мобильных экосистем: Разъясняет ли компания в доступной форме, что она проверяет, что приложения сторонних разработчиков в ее магазине приложений ограничиваются сбором пользовательских данных, необходимых для предоставления их услуг?
6. Для экосистем персональных цифровых помощников: Разъясняет ли компания в доступной форме, что она проверяет наличие в политике приватности навыков сторонних разработчиков, доступных в ее магазине навыков, информацию о сборе пользовательских данных этими навыками?
7. Для экосистем персональных цифровых помощников: Разъясняет ли компания в доступной форме, что она проверяет, что навыки сторонних

разработчиков в ее магазине навыков ограничиваются сбором пользовательских данных, необходимых для предоставления услуг навыков?

**Разъяснения по показателю**

Компании собирают широкий спектр личной информации пользователей — от личных данных и профилей учетных записей до действий пользователя и его местонахождения. Мы ожидаем, что компании будут четко раскрывать, какую информацию о пользователях они собирают и каким образом. Мы также ожидаем, что компании будут придерживаться принципа минимизации сбора данных и продемонстрируют, как этот принцип определяет их действия в отношении пользовательской информации. Если компании собирают несколько типов данных, мы ожидаем, что они предоставят подробную информацию о том, как они обрабатывают каждый тип. От мобильных экосистем и экосистем персональных цифровых помощников мы ожидаем предоставления информации о том, указаны ли в политике приватности приложений или навыков, доступных в магазине мобильных приложений или магазине навыков компании, какие сведения о пользователях собирают приложения или навыки и соответствуют ли эти политики принципам минимизации сбора данных.

**Потенциальные источники:**

- Политика приватности,
- Сайт компании или его раздел о защите данных или о сборе данных.

**P3(b). Пользовательские данные, полученные на основании логического вывода**

Компания должна в доступной форме разъяснять, какие пользовательские данные она получает на основании логического вывода.

*Параметры:*

1. Разъясняет ли компания в доступной форме, какие типы пользовательских данных она получает из собранной информации о пользователях на основании логического вывода?
2. Для каждого типа пользовательских данных, полученных логическим выводом, разъясняет ли компания в доступной форме, каким именно образом она пришла к таким выводам?
3. Разъясняет ли компания в доступной форме, что она ограничивает логическое выведение пользовательских данных исключительно данными, непосредственно необходимыми для предоставления ее услуг?

**Разъяснения по показателю**

Помимо сбора пользовательских данных, компании занимаются анализом больших данных, чтобы на основе собранной информации делать выводы или прогнозы о пользователях. Эти методы могут использоваться, чтобы делать выводы о предпочтениях или атрибутах пользователей (раса, пол, сексуальная ориентация и др.), об их мнениях (включая политические взгляды), а также для прогнозирования поведения потребителей. Логические умозаключения, нарушающие приватность пользователей и не поддающиеся проверке, не могут быть предсказаны, поняты или опровергнуты пользователями[30], если не будет достаточной прозрачности в процессе вывода новых данных, а также контроля со стороны пользователей.

Помимо информации о собираемых данных компании должны сообщать, какие выводы они делают и каким образом. Они также должны взять на себя обязательство делать выводы только о том, что уместно и необходимо для предоставления услуги. Например, компании не должны пытаться вывести принадлежность к религии или сексуальной ориентации, делать выводы о состоянии здоровья своих пользователей (например, путем отнесения их к той или иной категории аудитории на основании этих характеристик), если только эта информация не является непосредственно необходимой для предоставления услуги.

**Потенциальные источники:**

- Политика приватности компании, политика в отношении куки;
- Сайт компании или его раздел о защите данных или о сборе данных.

## P4. Предоставление пользовательских данных третьим лицам

Компания должна в четкой форме разъяснять, какой информацией о своих пользователях она делится и с кем.

*Параметры:*

1. Разъясняет ли компания в доступной форме, какими данными о своих пользователях она делится и с кем, предоставляя при этом разбивку по каждому типу данных?

[30] См.: Сандра Вахтер и Брент Миттельштадт, «Право на целесообразные выводы: Взгляд на закон о защите данных в эпоху больших данных и ИИ», 5 октября 2018 года. Columbia Business Law Review, 2019 (2), https://ssrn.com/abstract=3248829 [анг]

2. Разъясняет ли компания в доступной форме, с третьими сторонами каких типов она делится пользовательскими данными, с разбивкой по каждому типу данных?
3. Разъясняет ли компания в доступной форме тот факт, что она может выдать информацию о своих пользователях по запросу правительств или судебных органов?
4. Раскрывает ли компания в доступной форме названия всех третьих сторон, с которыми она делится пользовательскими данными, с разбивкой по каждому типу данных?
5. Для мобильных экосистем: Разъясняет ли компания в доступной форме, что она проверяет наличие информации в политике приватности приложений сторонних разработчиков в ее магазине приложений о том, какие пользовательские данные эти приложения передают третьим лицам?
6. Для мобильных экосистем: Разъясняет ли компания в доступной форме, что она проверяет наличие информации в политике приватности приложений сторонних разработчиков в ее магазине приложений о том, каким типам третьих сторон приложения передают пользовательскую информацию?
7. Для экосистем персональных цифровых помощников: Разъясняет ли компания в доступной форме, что она проверяет наличие информации в политике приватности навыков от сторонних разработчиков в ее магазине навыков о том, какие пользовательские данные эти навыки передают третьим лицам?
8. Для экосистем персональных цифровых помощников: Разъясняет ли компания в доступной форме, что она проверяет наличие информации в политике приватности навыков сторонних разработчиков в ее магазине навыков о том, какому типу третьих сторон навыки передают пользовательскую информацию?

**Разъяснения по показателю**

Компании собирают широкий спектр информации о пользователях — от личных данных и профилей учетных записей до действий в браузере и местоположения. Компании также часто передают эту информацию третьим лицам, включая рекламодателей, правительства и судебные органы. Мы ожидаем, что компании будут четко раскрывать, какой пользовательской информацией (по определению RDR) они делятся и с кем. Компании должны указать, делятся ли они информацией о пользователях с правительствами и коммерческими организациями. В отношении мобильных экосистем мы ожидаем, что компания будет четко раскрывать, указаны ли в политике приватности приложений, доступных в ее магазине приложений, сведения

о том, какую пользовательскую информацию приложения передают третьим лицам. Компании, управляющие экосистемами персональных цифровых помощников, должны требовать, чтобы сторонние навыки, доступные в их магазине навыков, четко раскрывали, какие типы пользовательской информации передаются, а также указывали типы третьих сторон, которым передается пользовательская информация.

**Потенциальные источники:**

- Политика приватности компании,
- Политика компании в отношении распространения данных и общению с третьими лицами.

## P5. Цели сбора, логического выведения и распространения пользовательских данных

Компания должна в доступной форме разъяснять, как именно она собирает, логически выводит и делится пользовательскими данными с другими.

*Параметры:*

1. Разъясняет ли компания в доступной форме, с какой целью она собирает данные о своих пользователях, с разбивкой по каждому типу данных?
2. Разъясняет ли компания в доступной форме, с какой целью она логически выводит данные о своих пользователях, с разбивкой по каждому типу данных?
3. Разъясняет ли компания в доступной форме, занимается ли она сопоставлением информации о пользователях разных сервисов компании? Если да, то с какой целью?
4. Разъясняет ли компания в доступной форме цели передачи данных о своих пользователях третьим сторона, с разбивкой по каждому типу данных?
5. Разъясняет ли компания в доступной форме, что ограничивается использованием данных своих пользователей только целями, с которыми эти данные были собраны или логически выведены?

**Разъяснения по показателю**

Мы ожидаем, что компании будут четко раскрывать цели сбора, распространения и вывода каждого типа пользовательских данных, которые они собирают, распространяют и логически выводят. Многие компании владеют или управляют различными продуктами и сервисами; и мы ожидаем, что компании будут четко раскрывать, как одна и та же пользовательская информация используется или

комбинируется на разных сервисах. Компании также должны придерживаться принципа ограничения использования — то есть публично заявлять в своей политике об использовании данных только в указанных целях в соответствии с Руководящими принципами ОЭСР по приватности [анг], Общим регламентом по защите персональных данных (GDPR [анг]) и другими нормативными документами в отношении как собираемой, так и получаемой посредством логического вывода пользовательской информации.

**Потенциальные источники:**

- Политика приватности компании

## P6. Хранение пользовательских данных

Компания должна в доступной форме разъяснять, как долго она хранит пользовательские данные.

*Параметры:*

1. Разъясняет ли компания в доступной форме, как долго она хранит пользовательские данные, с разбивкой по каждому типу данных?
2. Разъясняет ли компания в доступной форме, какие обезличенные пользовательские данные она хранит?
3. Разъясняет ли компания в доступной форме свои процессы обезличивания пользовательских данных?
4. Заявляет ли компания в доступной форме, что она удаляет все пользовательские данные после удаления пользователями своего аккаунта?
5. Раскрывает ли компания в доступной форме сроки, в течение которых она удаляет все пользовательские данные после удаления пользователями своего аккаунта?
6. Для мобильных экосистем: Разъясняет ли компания в доступной форме, что она проверяет наличие информации в политике приватности приложений сторонних разработчиков, доступных через ее магазин приложений, о сроках хранения пользовательской информации?
7. Для мобильных экосистем: Разъясняет ли компания в доступной форме, что она проверяет наличие заявления в политике приватности приложений сторонних разработчиков, доступных через ее магазин приложений, что при закрытии аккаунта или удалении приложения пользователем вся пользовательская информация будет удалена?

8. Для экосистем персональных цифровых помощников: Разъясняет ли компания в доступной форме, что она проверяет наличие информации в политике приватности навыков сторонних разработчиков, доступных через ее магазин навыков, о сроках хранения пользовательской информации?
9. Для экосистем персональных цифровых помощников: Разъясняет ли компания в доступной форме, что она проверяет наличие заявления в политике приватности навыков сторонних разработчиков, доступных через ее магазин навыков, что при закрытии аккаунта или удалении навыков пользователями вся пользовательская информация будет удалена?

**Разъяснения по показателю**

Мы ожидаем от компаний не только раскрытия того, какую информацию о пользователях они собирают и предоставляют третьим лицам, но также четкого указания сроков хранения информации и того, насколько тщательно удаляются идентификационные данные из хранимой ими персональной информации. В дополнение к этому у пользователей должна быть четкая информированность о том, что происходит с их данными в случае удаления ими своих учетных записей. В ряде случаев действующее законодательство может требовать от компаний хранения определенной информации в течение установленного срока. Компании должны четко информировать пользователей о наличии таких требований. Компании, принявшие на себя решение о хранении пользовательской информации в течение длительного периода времени, обязаны принять меры для обеспечения невозможности привязки такой информации к отдельным пользователям. Принимая во внимание продолжающиеся споры об эффективности процессов деидентификации и растущую сложность практики реидентификации, мы все же считаем деидентификацию положительным шагом, который могут предпринять компании для защиты приватности своих пользователей.

Если компаниями собирается несколько различных типов информации, мы ожидаем четкого информирования о продолжительности периода хранения информации каждого отдельного типа. В отношении мобильных экосистем и экосистем персональных цифровых помощников ожидается, что компании будут раскрывать информацию о наличии в политике приватности мобильных приложений или навыков, доступных в их магазинах приложений или навыков, информации о сроках хранения пользовательских данных и о том, подлежит ли удалению пользовательская информация в полном объеме в случае удаления пользователем приложения или навыка.

**Потенциальные источники:**

- Политика приватности компании,
- Сайт компании или его раздел о защите или сборе данных.

### P7. Контроль пользователей над своими данными

Компания должна в доступной форме разъяснять своим пользователям, каким образом они могут осуществлять контроль за сбором, выводом, хранением и использованием компанией их пользовательской информации.

*Параметры:*

1. Разъясняет ли компания в доступной форме факт наличия или отсутствия у пользователей возможности контролировать процесс сбора их пользовательской информации с разбивкой по каждому типу собираемых компанией пользовательских данных?
2. Разъясняет ли компания в доступной форме факт наличия или отсутствия у пользователей возможности удаления своей пользовательской информации с разбивкой по каждому типу собираемых пользовательских данных?
3. Для каждого типа пользовательской информации, которую компания выводит на основе собранных ею данных, четко ли компания объясняет возможность пользователей контролировать функцию вывода таких пользовательских данных?
4. Для каждого типа пользовательской информации, которую компания выводит на основе собранных ею данных, четко ли компания раскрывает возможность пользователей удалить такую пользовательскую информацию?
5. Сообщает ли компания в доступной форме, что она предоставляет пользователям возможность контролировать использование их персональных данных для таргетированной рекламы?
6. Сообщает ли компания в доступной форме, что таргетированная реклама отключена по умолчанию?
7. Сообщает ли компания в доступной форме, что она предоставляет пользователям возможность контролировать использование их пользовательской информации при разработке алгоритмических систем?
8. Сообщает ли компания в доступной форме, что она использует или не использует пользовательскую информацию для разработки алгоритмических систем по умолчанию?
9. Для мобильных экосистем и экосистем персональных цифровых помощников: Сообщает ли компания в доступной форме, что она

предоставляет пользователям возможность контроля функции геолокации устройства?

**Разъяснения по показателю**

Мы ожидаем, что компании будут четко информировать пользователей о возможностях контролировать сбор, хранение и вывод компанией информации о них. Предоставление пользователям возможности контроля над тем, какую информацию о них собирает, выводит и хранит компания, означает также предоставление пользователям возможности удалять определенные типы пользовательской информации, не требуя удаления всей учетной записи. Соответственно, мы ожидаем, что компании будут четко раскрывать информацию о том, есть ли у пользователей возможность удаления конкретных видов пользовательской информации. Помимо этого мы ожидаем, что компании предоставят пользователям возможность контроля над использованием их данных с целью размещения таргетированной рекламы и разработки алгоритмических систем. Таргетированная реклама требует масштабного сбора, хранения и вывода пользовательской информации, поэтому компании должны четко раскрывать, есть ли у пользователей возможность контролировать использование своих данных для подобных целей.

В отношении экосистем мобильных устройств и экосистем персональных цифровых помощников мы ожидаем, что компании будут четко раскрывать, какие возможности есть у пользователей для контроля над получением информации об их местоположении. Местоположение пользователя часто меняется, и многие пользователи носят свои мобильные устройства практически везде, что делает сбор подобного рода информации особенно уязвимым. Помимо этого, настройки местоположения в мобильных экосистемах и экосистемах персональных цифровых помощников влияют на доступ к информации о местоположении пользователя со стороны других продуктов и услуг. К примеру, мобильные приложения или навыки экосистемы персональных цифровых помощников могут предоставлять пользователям возможность управления данными о местоположении. Однако если устройство, на котором работают такие мобильные приложения или навыки, собирает геолокационные данные по умолчанию и не предоставляет пользователям возможности отключить эту функцию, пользователи могут быть лишены возможности накладывать ограничения на получение мобильными приложениями или навыками сведений об их местоположении. В связи с этим ожидается, что компании будут раскрывать информацию о том, какие возможности есть у пользователей при контроле процессов передачи устройствами данных об их местоположении.

**Потенциальные источники:**

- Политика приватности компании,

- Страница настроек аккаунта компании, страница настроек приватности,
- Центр поддержки компании.

### P8. Доступ пользователей к своим данным

Компании должны предоставить пользователям возможность получения всех своих пользовательских данных, имеющихся у компании.

*Параметры:*

1. Раскрывает ли компания в доступной форме информацию о том, что пользователи могут запросить копию своих пользовательских данных?
2. Сообщает ли компания в доступной форме, какую именно пользовательскую информацию могут получить пользователи?
3. Сообщает ли компания в доступной форме о возможности получения пользователями своей пользовательской информации в формате структурированных данных?
4. Сообщает ли компания в доступной форме о возможности получения пользователями располагаемой компанией общедоступной и приватной информации о них в полном объеме?
5. Сообщает ли компания в доступной форме о возможности у пользователей доступа к списку категорий рекламной аудитории, определенному для них компанией?
6. Сообщает ли компания в доступной форме, что пользователи могут получить в полном объеме всю информацию, которую компания может о них вывести?
7. Для мобильных экосистем: Сообщает ли компания в доступной форме, что она проверяет наличие информации в политике приватности приложений сторонних разработчиков, доступных через ее магазин приложений, о возможности получения пользователями своих хранящихся в таких приложениях данных в полном объеме?
8. Для экосистем персональных цифровых помощников: Сообщает ли компания в доступной форме, что она проверяет наличие информации в политике приватности навыков сторонних разработчиков, доступных через ее магазин навыков, о возможности получения пользователями своих хранящихся в навыках пользовательских данных в полном объеме?

**Разъяснения по показателю**

Пользователи должны иметь возможность получить всю свою пользовательскую информацию, находящуюся в распоряжении компаний: как общедоступную, так и внутреннюю. Сюда относится и та информация, которую компания задействовала для составления аналитических выводов или прогнозов в отношении пользователей. Мы ожидаем, что компании будут четко информировать пользователей о возможности получения такой информации, а также о том, какие данные содержатся в подобных материалах и в каких форматах пользователи могут их получить. Компании также должны предоставить пользователям возможность доступа к списку рекламных категорий, к которым они были причислены. В целях таргетирования рекламы компании, как правило, классифицируют каждого пользователя по разным целевым группам потребителей. Впоследствии рекламодатели могут выбрать, на какие категории аудитории они хотят ориентироваться. Пользователям должна быть доступна информация о том, к каким целевым группам потребителей их причислила компания на основании собранных сведений о пользователях или на основании предложенных о них выводов.

В отношении мобильных экосистем ожидается, что компания будет информировать пользователей о наличии в приложениях, доступных в ее магазине приложений, сведений о возможности получения пользователями всей хранящейся в приложении персональной информации. От компаний, управляющих магазинами навыков персональных цифровых помощников, ожидается установление обязательных требований, которым должны соответствовать навыки сторонних разработчиков, размещаемые на их платформах. Подобно тому, как мы ожидаем от самих компаний уведомления пользователей о возможности получения ими сведений об их собственных пользовательских данных, магазины навыков персональных цифровых помощников должны требовать от представленных в их магазинах навыков аналогичного уведомления пользователей.

**Потенциальные источники:**

- Политика приватности компании,
- Настройки аккаунта компании,
- Центр поддержки компании,
- Записи в блоге компании.

### P9. Сбор пользовательских данных у третьих лиц

Компания должна доступным образом разъяснить свою практику в отношении пользовательской информации, собираемой на сторонних веб-сайтах или в приложениях с помощью технических или нетехнических средств.

*Параметры:*

1. **Для цифровых платформ**: Разъясняет ли компания в доступной форме, какая пользовательская информация собирается ею с веб-сайтов третьих сторон с помощью технических средств?
2. **Для цифровых платформ**: Разъясняет ли компания в доступной форме, каким образом она собирает пользовательскую информацию от третьих сторон с помощью технических средств?
3. **Для цифровых платформ:** Четко ли компания указывает цель сбора информации о пользователях, полученной от третьих сторон с помощью технических средств?
4. **Для цифровых платформ**: Раскрывает ли компания в доступной форме информацию о сроках хранения пользовательских данных, полученных от третьих сторон с помощью технических средств?
5. **Для цифровых платформ**: Сообщает ли компания в доступной форме о принятии во внимание генерируемых пользователями сообщений о нежелании сбора их данных?
6. Разъясняет ли компания в доступной форме, какая пользовательская информация собирается третьими сторонами с помощью нетехнических средств?
7. Разъясняет ли компания в доступной форме, каким образом она собирает пользовательскую информацию от третьих сторон с помощью нетехнических средств?
8. Четко ли компания указывает цель сбора информации о пользователях, полученной от третьих сторон с помощью нетехнических средств?
9. Раскрывает ли компания в доступной форме информацию о сроках хранения пользовательских данных, полученных от третьих сторон с помощью нетехнических средств?

**Разъяснения по показателю**

Мы ожидаем, что компании будут раскрывать собираемую посредством третьих сторон информацию о пользователях. Сюда относится информация, собираемая с веб-сайтов или приложений сторонних разработчиков с помощью технических средств - например, с помощью файлов cookie, плагинов или виджетов, а также с помощью нетехнических средств - например, в рамках договорных соглашений. Данные о пользователях, собираемые с помощью нетехнических средств, в том числе в рамках договорных соглашений, могут стать частью «цифрового досье», которое компании могут вести в отношении своих пользователей и которое затем может стать базой для вывода и обмена сведениями о пользователях. Компании должны быть прозрачны и

подотчетны в отношении подобных практик, чтобы пользователи могли точно знать, отслеживаются ли их действия компаниями и каким именно образом (в том числе когда лицо не посещают сайт компании-собственника или не является пользователем определенной услуги или платформы).

**Потенциальные источники:**

- Политика приватности компании,
- Политика компании в отношении сторонних разработчиков или куки.

## P10. Процесс реагирования на требования о выдаче пользовательской информации

### P10(a). Процесс реагирования на правительственные требования о выдаче пользовательской информации

Компания должна в доступной форме отчитываться о процессе реагирования на требования властей о предоставлении пользовательской информации.

*Параметры:*

1. Отчитывается ли компания в доступной форме о процессе реагирования на внесудебные требования властей?
2. Отчитывается ли компания в доступной форме о процессе реагирования на судебные решения?
3. Отчитывается ли компания в доступной форме о процессе реагирования на требования властей иностранных государств?
4. Разъясняет ли компания в доступной форме правовые основания, на которых она может выполнить требование властей?
5. Разъясняет ли компания в доступной форме, что она проводит должную осмотрительность при принятии решения о том, как отреагировать на требования властей?
6. Обязуется ли компания противостоять неправомерным или чрезмерно широким требованиям властей?
7. Располагает ли компания изложенным в доступной форме руководством или примерами реализации своего процесса реагирования на требования властей?

**Разъяснения по показателю**

Компании часто получают от правительств требования о предоставлении данных пользователей. Такие требования могут исходить от органов исполнительной или судебной власти (как внутренних, так и зарубежных). Ожидается, что компании будут публично раскрывать свои процессы реагирования на подобные требования и юридические основания для выполнения требований, а также заявлять о четком намерении противостоять необоснованным или чрезмерным требованиям.

В ряде случаев законодательство может препятствовать разглашению компанией информации, упомянутой в материалах настоящего показателя. В каждом отдельном случае подобные ситуации будут задокументированы исследователями, но компания потеряет значительную часть оценки по показателю в случае несоответствия всем другим вышеперечисленным стандартам. Речь идет о ситуациях, когда законодательство препятствует компании в стремлении внедрения передовых практик. Поэтому мы призываем компании выступать за принятие законов, которые позволят им в полной мере соблюдать права пользователей на свободу самовыражения и неприкосновенность частной жизни.

**Потенциальные источники:**

- Отчет компании о прозрачности,
- Руководство компании по общению с органами правопорядка,
- Политика приватности,
- Отчет компании об устойчивом развитии,
- Записи в блоге компании.

### P10(b). Процесс реагирования на частные запросы о предоставлении пользовательских данных

Компания должна в доступной форме отчитываться о процессе реагирования на частные запросы о предоставлении пользовательских данных.

*Параметры:*

1. Раскрывает ли компания в доступной форме свои процессы реагирования на частные запросы о предоставлении пользовательских данных?
2. Разъясняет ли компания в доступной форме основания, на которых она может удовлетворить запросы, поступившие в частном порядке?
3. Разъясняет ли компания в доступной форме, что она проводит должную осмотрительность при принятии решений о том, как отреагировать на запросы, поступившие в частном порядке?

4. Обязуется ли компания противостоять неправомерным или чрезмерным запросам, поступившим в частном порядке?
5. Располагает ли компания изложенным в доступной форме руководством или примерами реализации процесса реагирования на запросы, поступившие в частном порядке?

**Разъяснения по показателю**

Компании все чаще получают частные запросы на предоставление пользовательских данных. Зачастую речь идет о запросах на получение данных о пользователях от неправительственных организаций - запросах, которые не сопряжены с каким-либо официальными процессуальными действиями. По данным Фонда Викимедиа, публикующего отчеты о прозрачности [анг] с данными о количестве полученных запросов такого рода, частные запросы на предоставление сведений о пользователях касаются, например, случаев, когда какая-либо компания направляет письмо или обращение по электронной почте с просьбой предоставить «непубличную информацию» об одном из пользователей. Информация может включать IP-адрес или адрес электронной почты пользователя.

В соответствии с данным показателем предполагается, что компании будут раскрывать свои процессы рассмотрения запросов подобного рода. Компании должны раскрывать основания для исполнения подобных требований, а также заявлять о четком намерении противостоять завышенным требованиям.

**Потенциальные источники:**
- Отчет компании о прозрачности,
- Политика компании по взаимодействию с правоохранительными органами,
- Политика приватности компании,
- Записи в блоге компании.

## P11. Данные о запросах на выдачу пользовательских данных

### P11(a). Данные о правительственных запросах на выдачу пользовательских данных

Компании должны с постоянной периодичностью публиковать данные о требованиях властей предоставить им пользовательские данные.

*Параметры:*

1. Предоставляет ли компания данные о количестве полученных требований властей такого рода с разбивкой по странам?
2. Предоставляет ли компания данные о количестве полученных правительственных запросов на хранящуюся пользовательскую информацию и на доступ к коммуникациям в режиме реального времени?
3. Предоставляет ли компания данные о количестве затронутых таким образом аккаунтов?
4. Приводит ли компания данные о том, какой характер носит требование: предоставление коммуникационного контента, неконтента или и того, и другого?
5. Обозначает ли компания конкретные правовые каналы или процесса, на основании которых предъявляются требования правоохранительных органов и органов национальной безопасности?
6. Включает ли компания данные о правительственных запросах, поступающих на основании судебных постановлений?
7. Приводит ли компания данные о количестве удовлетворенных ею правительственных запросов с разбивкой по категориям?
8. Приводит ли компания данные о том, какие виды правительственных запросов ей запрещено раскрывать в соответствии с законом?
9. Предоставляет ли компания такие данные не реже чем с ежегодной периодичностью?
10. Можно ли экспортировать полученные от компании данные в виде структурированного файла данных?

**Разъяснения по показателю**

Предполагается, что компании будут регулярно публиковать данные о количестве и видах получаемых ими подобных запросов, равно как и о количестве удовлетворенных запросов. Компании должны предоставлять данные о полученных ими запросах с указанием стран (включая запросы от правительств собственных стран и иностранных государств) и видов государственных органов (включая правоохранительные и судебные инстанций). Предполагается, что в раскрываемой компаниями информации будет указано количество и тип полученных запросов, а также количество удовлетворенных требований.

Следует признать, что в некоторых случаях законодательство не позволяет компаниям разглашать информацию о запросах властей на предоставление пользовательских данных. Предполагается, что в подобных случаях компании должны информировать о видах правительственных запросов, разглашение которых не допускается в соответствии с действующим законодательством. Компании должны

представлять подобные отчеты ежегодно и обеспечивать возможность экспорта информации в виде структурированного файла данных.

В ряде случаев законодательство может препятствовать разглашению компанией информации, упомянутой в материалах настоящего показателя. К примеру, предполагается, что компании будут публиковать точные данные, а не диапазоны значений. Однако следует признать, что законодательство в некоторых случаях препятствует подобным действиям со стороны компаний, поэтому в каждом отдельном случае подобные ситуации будут задокументированы исследователями. Тем не менее, компания потеряет значительную часть оценки в случае несоответствия всем другим вышеперечисленным стандартам. В данном случае речь идет о ситуации, когда законодательство препятствует компании в стремлении внедрения передовых практик. Поэтому мы призываем компании выступать за принятие законов, которые позволят им в полной мере соблюдать права пользователей на свободу самовыражения и неприкосновенность частной жизни.

**Потенциальные источники:**

- Отчет компании о прозрачности,
- Отчет компании о взаимодействии с органами правопорядка,
- Отчет компании об устойчивом развитии.

### P11(b). Данные о частных запросах на выдачу пользовательских данных

Компания должна с постоянной периодичностью публиковать данные о частных запросах на предоставление пользовательской информации.

*Параметры:*

1. Предоставляет ли компания данные о количестве полученных частных запросов на предоставление пользовательской информации?
2. Указывает ли компания количество удовлетворенных частных запросов о выдаче пользовательских данных?
3. Предоставляет ли компания на рассмотрение такие данные не реже одного раза в год?
4. Можно ли экспортировать полученные от компании данные в виде структурированного файла данных?

**Разъяснения по показателю**

Компании все чаще получают частные запросы на предоставление пользовательских данных. Зачастую речь идет о запросах на получение данных о пользователях от

неправительственных организаций - запросах, которые не сопряжены с каким-либо официальными процессуальными действиями. По данным Фонда Викимедиа, публикующего отчеты о прозрачности [анг] с данными о количестве полученных запросов такого рода, частные запросы на предоставление сведений о пользователях касаются, например, случаев, когда какая-либо компания направляет письмо или обращение по электронной почте с просьбой предоставить «непубличную информацию» об одном из пользователей. Информация может включать IP-адрес или адрес электронной почты пользователя.

Помимо публикации компаниями данных о получаемых ими запросах от властей, они должны также публиковать данные о полученных ими (и удовлетворенных) частных запросах на предоставление информации о пользователях. Предполагается, что компании будут на постоянной основе публиковать данные о количестве и типе полученных запросов, а также о количестве удовлетворенных ими запросов.

Компании должны представлять подобные отчеты ежегодно и обеспечивать возможность экспорта информации в виде структурированного файла данных.

**Потенциальные источники:**

- Отчет компании о прозрачности,
- Отчет компании об устойчивом развитии,
- Корпоративный отчет о социальной ответственности.

## P12. Уведомление пользователей о запросах со стороны третьих лиц

Компания должна в максимально допустимой с точки зрения закона степени уведомлять пользователей о том, что их пользовательская информация затребована государственными органами и прочими третьими лицами.

*Параметры:*

1. Сообщает ли компания в доступной форме, что она уведомляет соответствующих пользователей в случае поступления запроса от государственных органов (в т. ч. судов или правоохранительных органов) на предоставление пользовательской информации?
2. Сообщает ли компания в доступной форме, что она уведомляет соответствующих пользователей в случае поступления частного запроса на предоставление пользовательской информации?

3. Раскрывает ли компания в доступной форме информацию о тех или иных обстоятельствах, при которых уведомление пользователей невозможно, и указывает ли она виды государственных запросов, о которых она в соответствии с действующим законодательством не может уведомить пользователей?

**Разъяснения по показателю**

Ожидается, что компании будут четко информировать пользователей о своих обязательствах по их уведомлению в случаях поступления запросов от третьих лиц о предоставлении пользовательских данных. Следует отметить что такое уведомление может быть невозможным в рамках проведения следственных действий. Ожидается, что компания проинформирует о типах запросов, раскрытие информации по которым запрещено действующим законодательством.

**Потенциальные источники:**

- Отчет компании о прозрачности,
- Политика компании по взаимодействию с правоохранительными органами,
- Политика приватности компании,
- Политика компании в области прав человека.

## P13. Проверка безопасности

Для обеспечения безопасности своих продуктов и услуг компания должна четко раскрывать информацию о своих организационных процессах.

*Параметры:*

1. Сообщает ли компания в доступной форме о наличии систем ограничения и контроля доступа сотрудников к пользовательской информации?
2. Сообщает ли компания в доступной форме о наличии отдела безопасности, который проводит проверку безопасности продуктов и услуг компании?
3. Раскрывает ли компания в доступной форме информацию о проведении аудита на предмет безопасности своих продуктов и услуг с привлечением сторонних подрядчиков?

**Разъяснения по показателю**

В связи с тем, что компании обрабатывают и хранят огромные объемы пользовательских данных, необходимо предусмотреть четкие меры безопасности для обеспечения сохранности этих данных. Ожидается, что в отчетности компаний будет четко указано о наличии систем контроля и ограничения доступа сотрудников к пользовательским данным. Помимо этого предполагается обязательное предоставление компаниями информации о привлечении внутренних и внешних специалистов по безопасности для проведения аудита безопасности своих продуктов и услуг.

**Потенциальные источники:**

- Политики приватности компании,
- Руководство компании по безопасности.

## P14. Устранение уязвимостей безопасности

Компания должна устранять уязвимости системы безопасности по мере их обнаружения.

*Параметры:*

1. Сообщает ли компания в доступной форме о наличии у нее соответствующего механизма, с помощью которого специалисты по безопасности могут сообщать об обнаруженных ими уязвимостях?
2. Сообщает ли компания в доступной форме о сроках, в течение которых рассматриваются сообщения об уязвимостях?
3. Обязуется ли компания не преследовать в судебном порядке специалистов, сообщающих об уязвимостях в соответствии с условиями механизма информирования компании?
4. Для мобильных экосистем и экосистем персональных цифровых помощников: Сообщает ли компания отчетливо, что обновления программного обеспечения, программные патчи системы безопасности, надстройки или расширения загружаются по зашифрованному каналу?
5. Для мобильных экосистем и телекоммуникационных компаний: Четко ли компания раскрывает информацию о том, какие именно изменения она внесла в мобильную операционную систему, если таковые имеются?
6. Для мобильных экосистем, экосистем персональных цифровых помощников и телекоммуникационных компаний: Четко ли компания раскрывает информацию о том, какое воздействие, если таковое имеется, оказывают

изменения на возможность рассылки пользователям обновлений системы безопасности?

7. Для мобильных экосистем и экосистем персональных цифровых помощников: Сообщает ли компания четкую дату, до которой она будет продолжать предоставлять обновления безопасности для устройства / операционной системы?
8. Для мобильных экосистем и экосистем персональных цифровых помощников: Обязуется ли компания предоставлять обновления безопасности для операционной системы и другого критически важного программного обеспечения в течение как минимум пяти лет после выпуска?
9. Для мобильных экосистем, экосистем персональных цифровых помощников и телекоммуникационных компаний: Если компания использует операционную систему, адаптированную из уже существующей системы, обязуется ли компания предоставлять исправления безопасности в течение одного месяца после того, как будет объявлено об обнаружении уязвимости?
10. Для экосистем персональных цифровых помощников: Четко ли компания раскрывает информацию о том, какие изменения в операционную систему персонального цифрового помощника она внесла, если таковые имеются?
11. Для экосистем персональных цифровых помощников: Четко ли компания раскрывает, какое воздействие, если таковое имеется, оказывают подобные изменения на ее возможность рассылки пользователям обновлений системы безопасности?

**Разъяснения по показателю**

Компьютерный код не совершенен. В случае обнаружения уязвимостей, подвергающих риску пользователей и их данные, необходимо принять меры по их устранению. Сюда относится предоставление пользователям возможности сообщать компании о любых обнаруженных ими уязвимостях. Особенно важно, на наш взгляд, обеспечение компаниями предоставления пользователям четких указаний относительно порядка и сроков обновления системы безопасности. Помимо этого, поскольку телекоммуникационные провайдеры могут изменять мобильные операционные системы с открытым исходным кодом, ожидается, что компании будут раскрывать информацию, влияющую на возможность пользователя получать доступ к критически важным обновлениям.

**Потенциальные источники:**

- Политики приватности компании,
- Руководство компании по безопасности,
- Форумы поддержки компании.

## P15. Нарушение сохранности данных

Компания должна публично раскрывать информацию о своих процессах реагирования на нарушение сохранности данных.

*Параметры:*

1. Сообщает ли компания в доступной форме, что при нарушении сохранности данных она без промедления уведомит об этом соответствующие органы?
2. Четко ли раскрывает компания процесс уведомления затронутых подобным образом субъектов?
3. Сообщает ли компания в доступной форме, какие шаги будут предприняты для устранения последствий нарушения сохранности данных для пользователей?

**Разъяснения по показателю**

Компании должны иметь четко регламентированные процессы по устранению последствий нарушения сохранности данных и ясную политику уведомления затронутых пользователей. Принимая во внимание, что утечки данных могут привести к значительным угрозам финансовой или личной безопасности человека, а также к разглашению приватной информации, компании необходимо обнародовать информацию о подобных процедурах. В таком случае пользователи смогут осознанно принимать решения и учитывать потенциальные риски, прежде чем подписываться на какие-либо услуги компании или предоставлять ей свои данные.

Ожидается также, что официальная политика компании в отношении порядка ее действий в случае нарушения безопасности данных, если таковое произойдет, будет опубликована предварительно, до возникновения подобного события.

**Потенциальные источники:**

- Условия использования компании или политика приватности,
- Руководство компании по безопасности.

## P16. Шифрование пользовательской коммуникации и приватного контента (цифровые платформы)

Компании следует обеспечить шифрование пользовательской переписки и частного контента, с целью предоставления пользователям контроля над тем, кто имеет доступ к этому контенту.

*Параметры:*

1. Сообщает ли компания в доступной форме, что передача сообщений между пользователями зашифрована по умолчанию?
2. Сообщает ли компания в доступной форме, что передача сообщений между пользователями осуществляется с использованием уникальных ключей шифрования?
3. Сообщает ли компания в доступной форме, что для защиты своего приватного контента пользователи могут использовать сквозное или полнодисковое шифрование (если таковое предусмотрено)?
4. Сообщает ли компания в доступной форме, что сквозное или полнодисковое шифрование используется по умолчанию?

**Разъяснения по показателю**

Шифрование данных является важным инструментом для защиты свободы самовыражения и приватности. Специальный докладчик ООН по вопросу о защите права на свободу мнений и их свободное выражение совершенно безоговорочно заявил, что шифрование данных и анонимность имеют важное значение для обеспечения соблюдения и защиты прав человека[31]. Ожидается, что компании будут четко информировать о наличии шифрования пользовательских коммуникаций по умолчанию, о защите передачи данных при помощи «совершенной прямой секретности», о наличии у пользователей возможности подключения сквозного шифрования, а также о том, включено ли оно по умолчанию. В отношении мобильных экосистем и экосистем персональных цифровых помощников ожидается, что компании будут четко раскрывать информацию о наличии функции полнодискового шифрования.

**Потенциальные источники:**

- Условия предоставления услуг компании или политика приватности,
- Руководство компании по безопасности,
- Центр поддержки,
- Отчет компании об устойчивом развитии,
- Официальный блог компании и/или пресс-релизы.

[31] Доклад о шифровании, анонимности и основном механизме защиты прав человека, *Управление Верховного комиссара ООН по правам человека* https://www.ohchr.org/en/issues/freedomopinion/pages/callforsubmission.aspx [анг]

## P17. Безопасность аккаунтов (цифровые платформы)

Компании должна содействовать пользователям в обеспечении защищенности их аккаунтов.

*Параметры:*

1. Сообщает ли компания в доступной форме об использовании передовых способов аутентификации для предотвращения незаконного доступа?
2. Сообщает ли компания в доступной форме о возможности просмотра пользователями недавней активности своего аккаунта?
3. Сообщает ли компания в доступной форме об уведомлении пользователей о любых подозрительных действиях и возможном несанкционированном доступе к их аккаунтам?

**Разъяснения по показателю**

Компании должны оказывать пользователям поддержку в обеспечении информационной безопасности их аккаунтов. Компании должны четко информировать об использовании передовых методов аутентификации для предотвращения несанкционированного доступа к учетным записям и данным пользователей. Ожидается, что компании также предоставят пользователям инструменты, которые позволят им самостоятельно обеспечить защищенность своих аккаунтов и своевременно распознавать случаи несанкционированного доступа.

**Потенциальные источники:**

- Центр безопасности компании,
- Страницы поддержки компании или поддержка сообщества,
- Страница настроек аккаунта компании,
- Блог компании.

## P18. Информирование и просвещение пользователей о потенциальных рисках

Компания должна разместить информацию, направленную на поддержку защиты пользователей от угроз в сфере кибербезопасности.

*Параметры:*

1. Публикует ли компания практические материалы с целью просвещения пользователей о способах защиты от угроз в сфере кибербезопасности, связанных с предлагаемыми ею продуктами или услугами?

**Разъяснения по показателю**

Компании, располагающие огромным массивом персональных данных пользователей, часто становятся мишенью для злоумышленников. В связи с этим компаниям следует оказывать пользователям необходимую поддержку с целью их самозащиты от подобных рисков. В частности, могут быть опубликованы рекомендации о способах расширенной аутентификации учетных записей или настройке параметров приватности; о защите от вредоносных программ, фишинга и атак с применением методов социальной инженерии; о том, как избежать травли или преследования в Интернете; о том, что такое «безопасное посещение сайтов». Компании должны предоставлять подобные рекомендации, используя понятный язык, в идеале в сочетании с наглядными визуальными материалами, с целью помочь пользователям понять характер тех рисков, с которыми они могут столкнуться. Такие материалы могут быть представлены в различных вариантах: в виде рекомендаций, инструкций, методических пособий, FAQ или иных материалов, изложенных легко воспринимаемым пользователями способом.

**Потенциальные источники:**

- Центр безопасности компании,
- Страницы поддержки компании или поддержка сообщества,
- Блог компании.

## Глоссарий

***Примечание:*** *Это не исчерпывающий глоссарий. Содержащиеся в нем определения и объяснения были написаны специально для использования исследователями при оценке компаний из сегмента ИКТ (информационно-коммуникационные технологии) по показателям данного проекта.*

**Автоматизированное принятие решений** — технология, позволяющая принимать решения без необходимости осуществления надзора или участия человека в процессе принятия решений, например, с помощью искусственного интеллекта или алгоритмов.

**Автоматический флаг** — флаг, источником которого является алгоритмическая система. См. также: флаг, созданный человеком.

**Аккаунт / пользовательский аккаунт** — набор данных, связанных с конкретным пользователем компьютерной системы, сервиса или платформы. Пользовательский аккаунт состоит как минимум из имени пользователя и пароля, при помощи которых пользователь получает доступ к своим данным.

**Аккаунт с ограниченными возможностями / ограничение пользовательского аккаунта** — ограничение, заморозка, деактивация или удаление аккаунта конкретного пользователя или его возможностей.

**Алгоритм** — набор инструкций, используемый при обработке информации и выдаче данных согласно условиям инструкции. Может быть как простейшим фрагментом кода, так и невероятно сложными, «способными рассчитывать тысячи переменных по миллионам элементов данных». В контексте интернет-, мобильных и телекоммуникационных компаний некоторые алгоритмы — в силу своей сложности, объемов и типов обрабатываемых пользовательских данных, а также возложенной на них функции принятия решений — имеют серьезное влияние на права человека пользователей, включая право на свободу выражения и приватность. См: “Algorithmic Accountability: A Primer,” Data & Society, https://datasociety.net/wp-content/uploads/2018/04/Data_Society_Algorithmic_Accountability_Primer_FINAL-4.pdf.

**Алгоритмическая система** — система, использующая алгоритмы, машинное обучение и/или смежные технологии для автоматизации, оптимизации и/или персонализации процессов принятия решений.

**Алгоритмическое курирование контента, рекомендации и/или система ранжирования** — система, использующая алгоритмы, машинное обучение и другие технологии автоматизированного принятия решений для организации, формирования и управления контентом и информацией на платформе таким образом, при котором контент персонализируется для каждого пользователя.

**Анонимизированные данные** — данные, никак не связанные с другой частью информации, которая может позволить идентифицировать пользователя.

Расширительный характер этого определения, используемого проектом «Рейтинг цифровых прав», необходим для отражения нескольких фактов. Во-первых, опытные аналитики могут деанонимизировать большие массивы данных, что делает почти все обещания анонимизации недостижимыми. По сути любые данные, привязанные к «анонимному идентификатору», не являются анонимными. Чаще всего это псевдоанонимные данные, которые могут быть связаны с личностью пользователя вне сети. Во-вторых, метаданные могут быть столь же или более показательными в отношении связей и интересов пользователя, нежели данные о контенте; поэтому эти данные представляют жизненно важный интерес. В-третьих, организации, имеющие доступ ко многим источникам данных (например, брокеры данных и правительства), могут объединить два или более источников данных, чтобы раскрыть информацию о пользователях. Таким образом, искушенные субъекты могут использовать кажущиеся анонимными данные, чтобы составить более полное представление о пользователе.

**Апелляция / обжалование** — применительно к целям RDR под определение апелляций подпадают процессы, посредством которых пользователи требуют от компании официального изменения решения о модерации контента или об ограничении учетной записи.

**Бот** — автоматизированная учетная запись в Интернете, в которой все или почти все действия или сообщения не являются результатом деятельности человека.

**Ботнет** — скоординированная сеть ботов, действующих согласованно и под контролем одного и того же лица или организации.

**Взаимодействие** — взаимодействие между компанией и заинтересованными сторонами. Инициаторами могут выступать как компании, так и заинтересованные стороны, при этом взаимодействия могут принимать различные форматы, включая встречи и прочие виды коммуникации.

**Виджет** — часть программного кода, позволяющая пользователю или компании встраивать приложения и контент с одного сайта или сервиса на другой сторонний сайт или сервис. В некоторых случаях компании используют виджеты на сторонних сайтах и собирают информацию о посетителях этих сайтов без их ведома.

**Внедрение** — серия анонсов соответствующих продуктов, проходящая поэтапно в течение определенного времени; процесс предоставления конечным пользователям исправлений, обновлений и доработок программного обеспечения.

**Внесудебные требования властей** — запросы, исходящие от государственных органов внесудебной власти. Могут включать запросы от министерств, агентств, департаментов полиции, сотрудников полиции (действующих в официальном качестве) и других государственных учреждений, органов или организаций исполнительной власти.

**Вовлечение заинтересованных сторон** — взаимодействие между компанией и заинтересованными сторонами. Компании или заинтересованные стороны могут выступать инициаторами таких взаимодействий, осуществляемых в различных форматах, включая встречи, различные виды коммуникации и т. д.

**Возможность выбора**. Компания предоставляет пользователю четкий и понятный механизм, позволяющий отказаться от сбора, использования или передачи данных. Opt-in означает, что компания не будет собирать, использовать или передавать данные с определенной целью до тех пор, пока пользователи не дадут явный сигнал о своем желании такого развития событий. Opt-out означает, что компания использует данные с определенной целью по умолчанию, но откажется от такого использования, если пользователь сообщит об этом компании. Следует отметить, что такое определение является потенциально спорным, поскольку многие защитники конфиденциальности считают, что только opt-in представляет собой приемлемый контроль. Однако в рамках RDR мы решили считать opt-out формой осуществления контроля.

**Вредоносное программное обеспечение** — общий термин, относящийся к разным видам вредоносного программного обеспечения, в том числа вирусам, «червям», программам для вымогательства, запугивания, незаконного слежения и другим видам злонамеренных действий. Может принимать вид исполняемого кода, скриптов, активного контента или другого программного обеспечения.

**Высшее руководство** — генеральный директор и/или другие представители руководящего звена, перечисленные компанией на веб-сайте или в иных официальных документах, например, в годовом отчете. При отсутствии установленного в самой компании перечня руководителей высшего звена иные должности руководителей высшего звена и должности высшего уровня управления (например, исполнительный директор или старший вице-президент) считаются должностями высшего руководства.

**Геолокация** — определение реального географического местоположения объекта, например, источника радиолокационного сигнала, мобильного телефона или подключенного к Интернету компьютерного терминала. Геолокация относится как к практике определения местоположения, так и к фактическому определенному местоположению.

**Данные о местоположении** — информация от сети или сервиса о том, где находится телефон или устройство пользователя (например, на основании информации с базовых станций мобильной сети, GPS или Wi-Fi).

**Действия по модерации контента (модерация контента)** — процедура проверки пользовательского контента, размещенного на интернет-сайтах, в социальных сетях и других онлайн-ресурсах, с целью определения соответствия контента данному сайту, местности или юрисдикции. В результате этого процесса контент может быть удален или ограничен модератором, действующим в качестве представителя соответствующей платформы или сайта. В последнее время в дополнение к человеку-

модератору компании все чаще полагаются на алгоритмические системы для модерации контента и информации на своих платформах. Источник: Content moderation, Encyclopedia of Big Data, https://doi.org/10.1007/978-3-319-32001-4_44-1.

**Дискриминация** (применительно к индексу RDR) — иное, несправедливое отношение к отдельным людям, компаниям или продуктам. Источник: Cambridge Business English dictionary, https://dictionary.cambridge.org/dictionary/english/discrimination.

**Документация** — предоставление компанией доступа к записям, с которыми могут ознакомиться пользователи, например, к протоколу изменений в условиях предоставления услуг или документах о политике конфиденциальности.

**Доступ к связи в режиме реального времени** — слежка за переговорами или другими электронными сообщениями во время разговора или перехват данных в момент их передачи. Такое наблюдение также иногда называют прослушкой. Необходимо учитывать разницу между запросом на прослушивание и запросом на получение информации из хранилища данных. Прослушка дает правоохранительным органам право доступа к будущим сообщениям, в то время как запрос на сохраненные данные дает правоохранительным органам доступ к записям сообщений, имевших место в прошлом. Правительство США может получить доступ к коммуникациям в реальном времени в соответствии с разделами о прослушке и регистраторе набранных номеров Закона о конфиденциальности электронных коммуникаций; российское правительство может осуществить такие действия посредством Системы оперативно-розыскных мероприятий (СОРМ).

**Жалоба**. RDR заимствует свое определение понятия жалоба из Руководящих принципов ООН: «Субъективно воспринимаемая несправедливость с точки зрения представлений отдельного лица или группы о своем праве, в основе которого может лежать закон, контракт, прямо или косвенно выраженное обещание, обычная практика или общие представления ущемленных общин о справедливости».
Источник: Руководящие принципы предпринимательской деятельности в аспекте прав человека ООН, https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_ru.pdf

**Заинтересованные стороны** — лица, имеющие «долю» (интерес) в деятельности компании, поскольку ее действия или решения каким-либо образом влияют на них. Стоит обратить внимание, что заинтересованные стороны не являются правообладателями. Правообладатели - это лица, чьи права человека могут быть затронуты напрямую. Они взаимодействуют с компанией и ее продукцией и услугами на ежедневной основе, обычно в качестве сотрудников, клиентов или пользователей.

Помимо этого существуют различные виды заинтересованных сторон: те, на кого оказывается непосредственное влияние, и «опосредованные заинтересованные стороны», чья роль заключается в защите прав непосредственно заинтересованных сторон. К опосредованным заинтересованным сторонам относятся лица и организации, информированные о правообладателях и способные выступать от их

имени (организации гражданского общества, группы активистов, ученые, политики и лица, формирующие общественное мнение). Источник: Stakeholder Engagement in Human Rights Due Diligence: Challenges and Solutions for ICT Companies by BSR, BSR, Сентябрь 2014, стр.10. http://www.bsr.org/reports/BSR_Rights_Holder_Engagement.pdf.

**Замедление** — грубая форма формирования трафика, при которой оператор сети замедляет поток пакетов через сеть. Операторы мобильной связи могут дросселировать трафик для обеспечения лимитов данных. Для дополнительной информации см. Data throttling: Why operators slow down your connection speed, Open Signal, http://opensignal.com/blog/2015/06/16/data-throttling-operators-slow-connection-speed/.

**Запрет отслеживания (Do Not Track, DNT)** — установка в настройках браузера пользователя, которая указывает компаниям или третьим лицам запрет на «отслеживание» пользователя. Другими словами, каждый раз, когда пользователь загружает веб-сайт, все стороны, вовлеченные в выдачу страницы (которых часто много, в том числе рекламодатели), получают указание не собирать и не хранить какую-либо информацию о посещении пользователем этой страницы. Однако это всего лишь запрос вежливости, компания может его проигнорировать, что многие и делают.

**Изменения мобильной операционной системы** — изменения, внесенные в стоковую версию мобильной ОС. Они могут повлиять на основную функциональность, пользовательский опыт или процесс развертывания обновлений программного обеспечения. Основная функциональность - это наиболее важные функции или возможности продукта или услуги. Например, основная функциональность смартфона включает отправку и прием телефонных звонков, текстовых сообщений и электронных писем, загрузку и запуск приложений, а также доступ в Интернет. Это относится к смартфонам Android, кроме произведенных компанией Google.

**Инициатива с участием разных заинтересованных сторон** — заслуживающая доверия многосторонняя организация, которая помимо представителей отрасли включает и управляется членами как минимум трех других групп заинтересованных сторон: гражданского общества, инвесторов, ученых, широких представителей пользователей или клиентов, технического сообщества и/или правительства. Ее модель финансирования формируется из более чем одного типа источников (корпорации, правительства, фонды, общественные пожертвования и т. д.). Ее независимость, строгость и профессионализм соответствуют высоким стандартам, в ней принимают активное участие правозащитные организации, имеющие солидный опыт независимости от корпоративного и/или правительственного контроля. Глобальная сетевая инициатива (Global Network Initiative) является примером многосторонней инициативы, направленной на обеспечение свободы выражения мнений и неприкосновенности частной жизни в секторе ИКТ.

**Искусственный интеллект**. Искусственный интеллект имеет множество применений и значений. Для целей методологии RDR под искусственным интеллектом понимаются системы, осуществляющие или имитирующие функции, для выполнения которых, как правило, требуется наличие разума. В качестве примеров можно привести программное обеспечение для распознавания лиц, обработку естественного языка и прочие технологии, использование которых интернет-, мобильными и телекоммуникационными компаниями влияет на свободу самовыражения и право на неприкосновенность частной жизни пользователей. См: Privacy and Freedom of Expression in the Age of Artificial Intelligence, Privacy International, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf.

**Исследователь в сфере безопасности** — лицо, занимающееся изучением способов обеспечения безопасности технических систем и/или изучением угроз компьютерной и сетевой безопасности с целью нахождения путей их устранения.

**Категории рекламной аудиторий** — группы пользователей, определяемые для направления им таргетированной рекламы, и объединенные общими характеристиками и/или интересами согласно данным, которые компания собрала из пользовательской информации или вывела на основе заключений.

**Команда / программа** — определенное подразделение в компании, которое несет ответственность за соответствие продуктов или услуг компании (в данном случае принципам свободы самовыражения и/или неприкосновенности частной жизни).

**Контент** — информация, содержащаяся в передаче по каналам проводной, устной или электронной связи (например, разговор по телефону или лично, текст, написанный и переданный в SMS или по электронной почте).

**Контроль со стороны руководства**. Руководство компании или руководитель высшего звена непосредственно курирует вопросы, связанные со свободой выражения мнений и неприкосновенностью частной жизни.

**Критическое (программное) обновление** — выпущенное в массовом порядке устранение уязвимости, связанной с безопасностью конкретного продукта. Уязвимости в системе безопасности классифицируются по степени серьезности: критические, важные, умеренные или низкие.

**Куки (cookies)** — «веб-технология, позволяющая веб-сайтам распознавать ваш браузер. Изначально cookies были разработаны для того, чтобы на веб-сайтах можно было использовать онлайн-корзины для покупок, хранить заданные предпочтения или сохранять авторизацию на сайте. Они также позволяют отслеживать и составлять профили, чтобы сайты могли вас распознавать и узнавать больше о том, какие

страницы вы посещаете, какие устройства используете и каковы ваши интересы - даже если у вас нет учетной записи на этом сайте или вы не авторизованы в системе».
Источник: Surveillance Self Defense: Cookies, Electronic Frontier Foundation, https://ssd.eff.org/en/glossary/cookies.

**Курирование, рекомендации и/или ранжирование** — практика использования алгоритмов, машинного обучения и других автоматизированных систем принятия решений для управления, формирования и регулирования потока контента и информации, предоставляемой платформой, как правило, в персонализированном для каждого отдельного пользователя виде.

**Легко найти**. Условия предоставления услуг или политика конфиденциальности находятся на расстоянии одного-двух кликов от главной страницы компании или сервиса или расположены в логически обоснованном месте, где пользователи, скорее всего, смогут их легко обнаружить.

**Легко понять / в доступном изложении**. Компанией были предприняты шаги, чтобы помочь пользователям лучше разобраться в условиях предоставления услуг и политике конфиденциальности. Сюда входит, в частности, предоставление кратких описаний, подсказок или рекомендаций, разъясняющих значение условий, использование заголовков разделов, удобного для чтения размера шрифта или других графических элементов, помогающих пользователям понять документ, или изложение условий с использованием удобного для чтения синтаксиса.

**Логический вывод данных.** Компании имеют возможность с помощью аналитики больших данных и алгоритмических технологий принятия решений делать выводы и строить прогнозы о поведении, предпочтениях и частной жизни своих пользователей. Используя такие методы, можно получить сведения о предпочтениях или атрибутах пользователей (например, о расе, поле, сексуальной ориентации), мнениях (например, о политических взглядах) или предсказать поведение (в частности, для размещения рекламы). Поскольку нет достаточной прозрачности и контроля пользователей над выводом информации из данных, такие вмешательства в частную жизнь и не поддающиеся проверке выкладки не могут быть предвидены, осмыслены или опротестованы пользователями. См: Wachter, Sandra and Mittelstadt, Brent. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, Columbia Business Law Review, 2019(2), https://ssrn.com/abstract=3248829.

**Магазин навыков** — платформа, с помощью которой компания предоставляет для загрузки свои навыки, а также навыки, созданные сторонними разработчиками. Магазин навыков (или рынок навыков) — это разновидность платформы цифрового распространения компьютерного программного обеспечения.

**Магазин приложений** — платформа, посредством которой компания предоставляет для скачивания свои собственные приложения, а также приложения, созданные сторонними разработчиками. Магазин приложений (или рынок приложений) - это тип

цифровой платформы для распространения компьютерного программного обеспечения, зачастую в мобильном контексте.

**Метрики взаимодействия** — показатели, характеризующие степень популярности контента или аккаунта на платформе, например, подписчики, контакты, друзья, комментарии, лайки, ретвиты и т. д.

**Минимизация данных.** Согласно принципу минимизации данных компании должны ограничивать сбор информации о пользователях только той, которая уместна и необходима для достижения четко определенной цели. См. также: ограничение цели или использования.

**Многоуровневые документы политики** — условия предоставления услуг и политики приватности, разделенные на разделы с гиперссылками, облегчающими навигацию для пользователей.

**Мобильная экосистема** — неразделимый набор товаров и услуг, предоставляемых компанией мобильных устройств. Состоит из аппаратной части, операционной системы, магазина приложений и пользовательских аккаунтов.

**Навыки** — управляемые голосом возможности персонального цифрового помощника, позволяющие пользователям выполнять определенные задачи или взаимодействовать с онлайн-контентом с помощью устройств, оснащенных персональным цифровым помощником. Навыки экосистемы персонального цифрового помощника похожи на приложения экосистемы мобильных устройств: пользователи могут включать и отключать встроенные навыки или устанавливать созданные сторонними разработчиками навыки через магазины, аналогичные магазинам приложений.

**Надзор / надзирать**. Внутренние документы компании или процедуры принятия решений наделяют комитет, группу или лицо официальными полномочиями по надзору за определенной функцией. Эта группа или лицо несет ответственность за выполнение данной функции, и ее деятельность оценивается в зависимости от того, насколько группа или лицо справляется с этой функцией.

**Накопленные пользовательские данные** — информация о пользователе, которую компания получает либо непосредственно, либо от третьих сторон.

**Нарушение сохранности данных** — утечка данных, возникающая, когда постороннее лицо получает доступ к пользовательской информации, которую компания собирает, хранит или иным образом обрабатывает; утечка подвергает риску целостность, безопасность или конфиденциальность этой информации.

**Национальный документ** — официальный, выданный государством документ (с фотографией или без фотографии), который может быть использован для подтверждения личности человека. Таким документом может быть удостоверение личности, выданное государственным органом, или другой документ,

идентифицирующий человека по его фактическому адресу, семейному положению или принадлежности к сообществу. Сюда также относятся номера телефонов, которые во многих юрисдикциях связаны с личностью человека вне сети.

**Не-контент** — данные о факте коммуникации или о пользователе. Компании могут использовать различные термины для обозначения этих данных: метаданные, основная информация об абоненте, транзакционные данные, не относящиеся к контенту, данные учетной записи или информация о клиенте.

Закон США «О сохраняемых коммуникациях» (Stored Communications Act) определяет не-контент как «имя; адрес; записи местных и междугородних телефонных соединений или записи о времени и продолжительности сеансов; продолжительность обслуживания (включая дату начала) и типы используемых услуг; номер телефона или прибора или другой абонентский номер или идентификатор (включая любой временно присвоенный сетевой адрес); средства и источник оплаты за такое обслуживание (включая любую кредитную карту или номер банковского счета)». Руководство к закону ЕС «О защите данных» (European Union's Handbook on European Data Protection Law) гласит: «Конфиденциальность электронных сообщений относится не только к содержанию сообщения, но и к данным о трафике (информация о том, кто, с кем, когда и как долго общался) и местоположении (например, откуда были переданы данные)».
См: 18 U.S. Code § 2703. Required disclosure of customer communications or records, Cornell Law School Legal Information Institute, https://www.law.cornell.edu/uscode/text/18/2703.
Handbook on European data protection law, European Court of Human Rights, https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

**Нетехнические средства**. Компании могут получать информацию о пользователях нетехническими способами: например, посредством покупки, соглашения об обмене данными и других договорных отношений с третьими сторонами. Эти данные могут стать частью «цифрового досье», которое компании могут собирать на своих пользователей и которое может стать основой для вывода и обмена информацией о пользователях.

**Неформальные процессы** — процедуры или каналы, через которые правительство выдвигает требования или запросы на ограничение контента или аккаунтов. Применяются взамен официальных способов, таких как закон или постановление. Например, местный чиновник может отдать распоряжение или выразить недовольство по поводу определенного контента через неофициальный канал.

**Обезличенные (пользовательские) данные** — информация о пользователях, которую компании собирают и сохраняют, но только после удаления или сокрытия из нее любой идентифицирующей части. Это означает удаление явных идентификаторов, таких как имена, адреса электронной почты и любые выданные государством идентификационные номера, а также удаление таких идентификаторов,

как IP-адреса, файлы cookie и уникальные номера устройств.

**Обещание следовать политике** — публично доступное заявление, представляющее собой официальную политику компании, утвержденную на высшем уровне руководства компании.

**Обновление безопасности** — широко распространяемое исправление уязвимости, связанной с безопасностью конкретного продукта. Уязвимости системы безопасности оцениваются по шкале серьезности: критические, важные, умеренные или низкие.

**Обновление версии программы** — выпуск новой версии программного обеспечения, предлагающей значительные изменения или улучшения по сравнению с текущей версией.

**Ограничение контента** — действия компании, в результате которых объект пользовательского контента становится недоступным или трудно доступным на платформе или в сервисе. Эти действия могут включать полное удаление контента или принимать менее категоричную форму: скрытие контента только от определенных категорий пользователей (например, жителей какой-либо страны или лиц моложе определенного возраста), ограничение возможности пользователей в отношении взаимодействия с ним (например, сделать невозможным «лайк»), добавление к нему ответных высказываний (например, корректирующей информации на посты против вакцины) или уменьшение степени его продвижения, обеспечиваемого курирующими системами платформы.

**Ограничение цели или использования.** Согласно принципу использования или минимизации целевого назначения организации, обрабатывающие информацию о пользователе, должны указать цель этих действий и ограничить использование этой информации для любых других целей, если они не получили согласия от пользователя. См. также: Минимизация данных.

**Операционная система** — программный комплекс, обеспечивающий основную функциональность устройства: запланированное выполнение заданий, запуск приложений, управление периферийными устройствами. Мобильная операционная система управляет устройствами типа смартфона или планшета.

**Основной функционал** — наиболее важные функции или возможности продукта или услуги. Например, основную функцию смартфона составляют совершение и прием телефонных звонков, текстовых сообщений и электронных писем, загрузка и запуск приложений, а также доступ в Интернет.

**Отмечание** — процесс оповещения компании о том, что часть контента или аккаунт могут нарушать установленные компанией правила; сигнал, передающий данную информацию компании. Такой процесс может осуществляться как внутри платформы,

так и через внешний процесс. К числу флагов относятся пользователи, алгоритмические системы, сотрудники компаний, правительства и другие субъекты.

**Оповещение / оповещать.** Таким способом компания рассказывает своим пользователям нечто о своих продуктах или услугах.

**Оценка воздействия на права человек (ОВПЧ)** — систематическая комплексная проверке того, насколько продукты, сервисы и бизнес-практики компании воздействуют на свободу самовыражения и приватность ее пользователей.

Для получения дополнительной информации об оценке воздействия на права человека и оптимальные практики проведения такой оценки: https://business-humanrights.org/en/un-guiding-principles/implementation-tools-examples/implementation-by-companies/type-of-step-taken/human-rights-impact-assessments [анг]

Инструмент проверки соответствия стандартам прав человека Датского института по правам человека: https://hrca2.humanrightsbusiness.org [анг]

Руководство по проведению ОПВЧ от BSR: http://www.bsr.org/en/our-insights/bsr-insight-article/how-to-conduct-an-effective-human-rights-impact-assessment [анг]

Руководство для компаний сектора ИКТ из книги Майкла Сэмвея Business, Human Rights and the Internet: A Framework for Implementation: http://rankingdigitalrights.org/resources/readings/samway_hria [анг]

**Параметры таргетинга** — параметры, обычно устанавливаемые рекламодателем и определяющие, какой категории пользователей будет показан соответствующий рекламный контент. Могут включать демографические данные пользователей, местоположение, поведение, интересы, связи и другие пользовательские данные.

**Платформа**. Вычислительная платформа — в широком смысле это готовая среда, предназначенная для запуска на ней программного обеспечения или объекта программного кода с соблюдением существующих особенностей и соответствующих требований. Термин вычислительная платформа может обозначать различные уровни абстракции, включая аппаратную архитектуру, операционную систему (ОС) и библиотеки среды выполнения [1]. В совокупности можно сказать, что вычислительная платформа является фундаментом, на котором могут запускаться программы.

**Политика в отношении ботов** — документ, в котором изложены правила компании, регулирующие использование ботов для создания и распространения контента или выполнения других действий. Может быть частью условий предоставления услуг компании или другой нормативной документации.

**Политика в отношении рекламного контента** — документация, излагающая правила компании относительно рекламного контента, допустимого на ее платформе.

**Политика использования алгоритмических систем** — документация, описывающая практические методы компании, связанные с использованием алгоритмов, машинного обучения и систем автоматизированного принятия решений.

**Политика приватности** — документация, описывающая практику компании в отношении сбора и использования информации, особенно пользовательской.

**Политика развития алгоритмических систем** — документация, излагающая практику компании по вопросам разработки и тестирования алгоритмов, машинного обучения и систем автоматизированного принятия решений.

**Политика таргетирования рекламы** — документация, излагающая правила компании относительно параметров рекламного таргетинга, допустимого на ее платформе.

**Полнодисковое шифрование** — комплексное шифрование всех данных, хранящихся на физическом устройстве. Выполняется таким образом, что только пользователь может получить доступ к содержимому, предоставив сгенерированный пароль(и) и/или другие средства дешифровки (отпечаток пальца, код двухфакторной аутентификации, физический токен и т. д.).

**Пользователь** — лицо, использующее какой-либо продукт или услугу. Это относится как к лицам, размещающим или распространяющим контент в Интернете, так и к тем, кто стремится получить доступ к контенту или ознакомиться с ним. Применительно к показателям в категориях свободы выражения мнений сюда относятся и сторонние разработчики, создающие приложения, размещаемые или распространяемые посредством предлагаемых компанией продуктов или услуг.

**Пользователь с ограниченными правами / затронутый пользователь** — пользователь, чей контент был ограничен действиями модератора, или пользователь, связанный с определенным аккаунтом, чьи права были ограничены действиями модератора. Также применимо к некоторым ситуациям: пользователь, создавший флаг, на основании которого определенный контент или пользователь были подвергнуты модерации.

**Пользовательские данные** — любые данные, которые имеют отношение к идентифицируемому лицу или могут быть соотнесены с таким лицом путем совмещения совокупностей данных или использования методов анализа данных. Информация о пользователе может быть либо получена, либо рассчитана. Следует пояснить, что информация о пользователе — это любые данные, которые документально подтверждают характеристики и/или действия пользователя. Подобная информация может быть связана или не связана с определенной учетной записью пользователя. К такой информации относятся, в частности, личная переписка, пользовательский контент, предпочтения и настройки аккаунта, данные журналов и входа, данные о действиях или предпочтениях пользователя, полученные от третьих сторон путем отслеживания поведенческих факторов или посредством приобретенных данных, а также все типы метаданных. Информация о пользователе никогда не считается анонимной за исключением тех случаев, когда она используется исключительно в качестве источника для построения общих показателей (например,

количество активных ежемесячных пользователей). В качестве примера приведем утверждение: «У нашего сервиса 1 миллион ежемесячных активных пользователей». Утверждение содержит анонимные данные, поскольку не предоставляет достаточной информации, позволяющей установить, кто именно входит в это число пользователей.

**Пользовательское соглашение / Условия предоставления услуг / Положения и условия**. По утверждению EFF, условия предоставления услуг «часто обеспечивают необходимые базовые правила использования различных онлайн-сервисов» и представляют собой юридическое соглашение между компанией и пользователем. Компании могут принимать меры в отношении пользователей и их контента на основании положений, закрепленных в условиях предоставления услуг. Источник: Terms of (Ab)use, Electronic Frontier Foundation, https://www.eff.org/issues/terms-of-abuse.

**Прекращение или ограничение доступа к сети** — преднамеренное нарушение работы Интернета или электронных коммуникаций, включая телекоммуникационные услуги, такие как сотовая телефония и SMS. Включает в себя полное отключение всех услуг сотовой связи или Интернета в географической зоне и целенаправленную блокировку конкретных сервисов, таких как социальные сети или приложения для обмена сообщениями.

**Приложение** — самостоятельная программа или часть программного обеспечения, предназначенная для выполнения конкретных задач; программное приложение, скачанное пользователем на мобильное устройство.

**Приоритизация.** Приоритезация происходит, к примеру, когда оператор сети «управляет своей сетью таким образом, что это выгодно для определенного контента, приложений, услуг или устройств». Источник: Правила открытого Интернета Федеральной Комиссии США по связям, 2015 год, стр 7, https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf [анг]. Применительно к RDR: решение компании заблокировать доступ к определенному приложению, услуге или устройству.

**Программная заплатка (патч)** — часть программного обеспечения, предназначенная для обновления компьютерной программы или ее сопутствующих данных с целью исправления или улучшения. Сюда относится устранение уязвимостей в системе безопасности и других багов (такие исправления обычно называют багфиксами или устранением неполадок), а также усовершенствование удобства использования или производительности компьютерной программы, приложения или операционной системы.

**Протокол изменений** — протокол, отражающий конкретные изменения в документе; в данном случае в условиях предоставления услуг или в политике приватности.

**Программа для информаторов** — процесс, с помощью которого сотрудники компании могут сообщать о любых предполагаемых злоупотреблениях в компании, включая вопросы, связанные с правами человека. Как правило, такая программа

имеет вид анонимной «горячей линии», за работа которой обеспечивается под контролем руководителя отдела корпоративного регулирования или отдела по вопросам этики.

**Программа нулевого рейтинга.** Под нулевым рейтингом понимается практика невзимания платы с пользователей за данные, необходимые для доступа к определенным онлайн-сервисам или платформам. Нулевой рейтинг рассматривается как разновидность сетевого приоритета, подрывающего принцип сетевого нейтралитета.

**Прямая секретность / совершенная прямая секретность** — метод шифрования, часто используемый в сетевом трафике HTTPS и в приложениях для обмена сообщениями, при котором новая пара ключей генерируется для каждого сеанса или для каждого сообщения, которым обмениваются стороны (приложения для обмена сообщениями). Таким образом, если злоумышленник получит один ключ дешифрования, он не сможет расшифровать прошлые или будущие передачи или сообщения в переписке. Прямая секретность отличается от сквозного шифрования, при котором данные шифруются в состоянии «покоя» на удаленных серверах компании. См: Pushing for Perfect Forward Secrecy, Electronic Frontier Foundation, https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-important-web-privacy-protection.

**Прямо оповещать / прямое оповещение** — уведомление пользователей об изменениях или обновлениях политики компании, применяемой к конкретной услуге. Уведомление происходит непосредственно через услугу, в которой намечены изменения. Метод прямого уведомления может отличаться в зависимости от типа услуги. Для услуг, требующих наличия учетной записи пользователя, прямое уведомление может включать отправку электронного письма или SMS. Для услуг, не требующих учетной записи пользователя, прямое уведомление должно включать размещение заметного уведомления на главной веб-странице или платформе, через которую пользователи получают доступ к услуге.

**Протокол** — набор правил, регулирующих обмен или передачу данных между устройствами.

**Программное обновление (апдейт, программный патч)** — бесплатно загружаемое приложение или программный пакет, обеспечивающий исправление функций, которые работают не так, как предполагалось, или добавляющий незначительные программные улучшения и обеспечения совместимости. Обновление может также содержать обновления драйверов, которые улучшают работу оборудования или периферийных устройств или добавляют поддержку новых моделей периферийных устройств.

**Публичный архив** — публично доступный ресурс, содержащий предыдущие версии политики компании (например, условий предоставления услуг или политики конфиденциальности) или подробное объяснение всех изменений, вносимых в данную политику.

**Публичный архив запросов третьих сторон.** Прекрасно, когда компании публикуют информацию о полученных запросах, чтобы общественность имела лучшее представление о способах ограничения контента на платформе. Компании могут предоставлять информацию о полученных запросах в сторонний архив. Примером такого архива является Lumen (ранее Chilling Effects) — независимый исследовательский проект, управляющий общедоступной базой данных запросов на удаление онлайн-контента. Такой тип хранилища помогает исследователям и общественности получить представление о видах контента, запрашиваемого для удаления, а также лучше понимать легитимные и нелегитимные запросы. См https://cyber.harvard.edu/research/lumen [анг].

**Разработчик / сторонний разработчик** — физическое лицо (или группа лиц), создающее программу или приложение, которое распространяется через магазин приложений компании.

**Расшары / поделиться** — компания позволяет третьим сторонам получать доступ к информации о пользователе, бесплатно предоставляя эту информацию третьим лицам (общественности или другим пользователям), либо путем ее продажи третьим лицам.

**Реклама** — сообщение, за которое рекламодатель заплатил компании, чтобы та показывала его определенному сегменту своей аудитории. В состав рекламного сообщения входит не только рекламный контент, но и параметры, по которым производится таргетинг.

**Рекламная сеть** — компания или сервис, которые связывают рекламодателей с сайтами, готовыми разместить у себя рекламу. Ключевая функция рекламной сети состоит в сборе данных о предложениях на рынке рекламного пространства среди издателей (паблишеров), а также поиска для них соответствующего спроса среди рекламодателей.

**Рекламные технологии** — основанные на алгоритмах системы принятия решений, которые определяют, каким пользователям будет показано конкретное рекламное сообщение. Пользователи могут определяться по заданным рекламодателем параметрам или полностью автоматически.

**Рекламный контент** — любой контент, за который кто-то заплатил компании, чтобы она показывала его своим пользователям.

**Рекламодатель** — физическое или юридическое лицо, которое создало и/или заплатило за рекламный контент. Обычно рекламодатель определяет параметры таргетинга для каждого рекламного сообщения.

**Риски в области кибербезопасности** — ситуации, в которых безопасность, конфиденциальность или другие права пользователей могут оказаться под угрозой из-за действий злоумышленников (включая, но не ограничиваясь, преступниками, инсайдерами или национальными государствами), имеющих возможность незаконного

доступа к данным пользователей посредством хакерских, фишинговых или других мошеннических методов.

**Сбор / накопление** — все средства, с помощью которых компания может осуществлять сбор информации о пользователях. Например, компания может непосредственно собирать пользовательскую информацию в различных ситуациях, в том числе когда пользователи загружают контент для всеобщего доступа, предоставляют номера телефонов для проверки аккаунта, передают личную информацию в частной переписке и т. д. Компания также может собирать эту информацию косвенно, например, путем протоколирования лог-данных, сведений об учетной записи, а также метаданных и другой сопутствующей информации, которая описывает пользователей и/или документирует их действия.

**Сквозное шифрование**. При сквозном шифровании только отправитель и получатель могут прочитать содержимое зашифрованных сообщений. Сторонние лица, включая саму компанию, не смогут расшифровать содержимое.

**Совет директоров.** Контроль на уровне совета директоров должен включать в себя прямой надзор членов совета директоров за соблюдением принципов свободы выражения мнений и неприкосновенности частной жизни. Это не обязательно должен быть официальный комитет, но ответственность членов совета директоров по надзору за практикой компании в этих вопросах должна быть четко сформулирована и размещена на сайте компании.

**Создаваемые пользователями сигналы.** Многие компании позволяют пользователям отказаться от отслеживания путем настройки набора определенных компанией файлов cookie. Если пользователь удаляет файлы cookie в целях защиты своей приватности, его отслеживание тем не менее будет продолжаться до тех пор, пока он не изменит настройки файлов cookie на «отказ от использования». Помимо этого, для предотвращения отслеживания некоторые компании могут требовать от пользователя установления дополнения к браузеру. Эти распространенные сценарии являются примерами того, как пользователей вынуждают использовать методы, определяемые компанией, поэтому они не могут считаться полностью исходящими от пользователей. Сигнал же, созданный пользователем, исходит от самого пользователя и является универсальным сообщением о том, что его не следует отслеживать. На сегодняшний день наиболее распространенным вариантом пользовательского сигнала является установка «запрета на отслеживание» в настройках браузера (см. выше). Тем не менее, пользователи не должны быть ограничены в других способах сообщения о своем нежелании быть отслеживаемыми.

**Создатель флага** — физическое или юридическое лицо, которое уведомляет компанию о том, что часть контента или аккаунт могут нарушать правила компании. Такой процесс может происходить как внутри платформы, так и внешне. К создателям флагов относятся пользователи, алгоритмические системы, сотрудники компании, правительства, другие частные субъекты.

**Сохранение пользовательских данных.** Компания может накапливать данные, а затем удалять их. Если компания не удаляет данные, они сохраняются. Время между сбором и удалением данных является периодом хранения. Подобные данные могут соответствовать нашему определению информации о пользователе или являться анонимными. Следует учитывать, что подлинно анонимные данные никоим образом не могут быть связаны с пользователем, его личностью, поведением и предпочтениями, что наблюдается крайне редко.

Смежной тематикой является срок хранения. К примеру, компания может осуществлять сбор лог-данных на постоянной основе, но при этом вычищать (удалять) эти данные с периодичностью раз в неделю. В подобном случае период хранения данных составляет одну неделю. Тем не менее, если период хранения не указан, по умолчанию предполагается, что данные не подлежат удалению и период их хранения является неограниченным. В ряде случаев пользователям может быть удобно, чтобы их данные сохранялись на период активного пользования услугой, но при прекращении пользования услугой могли бы быть удалены. Например, пользователь может пожелать, чтобы социальная сеть сохраняла все его личные сообщения. Но при уходе из сети пользователь может желать, чтобы все его личные сообщения были удалены.

**Средства правовой защиты**. «Средства правовой защиты могут включать в себя принесение извинений, реституцию, реабилитацию, финансовую или иную компенсацию и карательные меры (уголовные или административные, например, штрафы), а также предупреждение причинения ущерба посредством, например, судебных запретов или обеспечения гарантий недопущения повторного нарушения. Процедуры предоставления средств правовой защиты должны быть беспристрастными, защищенными от коррупции и лишенными политических или иных посягательств на результат».
Источник: Отчет Специального представителя Генерального секретаря по вопросу о правах человека и транснациональных корпорациях и других предприятиях Джона Рагги. Руководящие принципы предпринимательской деятельности в аспекте прав человека: Осуществление рамок Организации Объединенных Наций в отношении «защиты, соблюдения и средств правовой защиты», 2011, стр. 22. http://business-humanrights.org/sites/default/files/media/documents/ruggie/ruggie-guiding-principles-21-mar-2011.pdf [анг]

**Структурированные данные** — «данные, находящиеся в определенных графах в составе записи или файла. Реляционные базы данных и электронные таблицы являются примерами структурированных данных. Хотя в отличии от записей в традиционных базах данных данные в XML-файлах не имеют фиксированного расположения, они, тем не менее, являются структурированными, поскольку данные помечены и могут быть точно идентифицированы. И наоборот, неструктурированные данные — это данные, которые не хранятся в зафиксированных местах. Это обычно относится к тексту в свободной форме, который встречается везде. Примерами могут служить документы текстовых редакторов, файлы PDF, сообщения электронной почты, блоги, веб-страницы и сайты социальных сетей».

Источник: PC Mag Encyclopedia. Структурированные данные: http://www.pcmag.com/encyclopedia/term/52162/structured-data [анг], неструктурированные данные: http://www.pcmag.com/encyclopedia/term/53486/unstructured-data [анг].

**Судебное решение** — постановления, вынесенные судом по уголовным, административным или гражданским делам.

**Таргетированная реклама / реклама на основе интересов / персонализированная реклама / программатическая реклама** — практика доставки адаптированных рекламных объявлений пользователям на основе их истории просмотров, информации о местоположении, профилей и активности в социальных сетях, а также демографических характеристик и других параметров. Таргетированная реклама опирается на широко распространенную практику сбора данных, которая может включать отслеживание действий пользователей в Интернете с помощью файлов cookie, виджетов и других инструментов отслеживания для создания детализированных характеристик пользователя.

**Технические средства.** Компании используют различные технологии, включая файлы cookie, виджеты и кнопки, для отслеживания активности пользователей на своих и сторонних сервисах и сайтах. Например, компания может встраивать контент на сайт третьей стороны и собирать информацию о пользователе, когда пользователь ставит лайк или иным образом взаимодействует с контентом.

**Требование.** Требование со стороны компании может быть выдвинуто в момент регистрации аккаунта пользователя или позже.

**Требования властей** — требования государственных министерств и ведомств, правоохранительных органов, а также судебные решения по уголовным и гражданским делам.

**Третья сторона** — лицо (организация), не являющееся компанией или пользователем ее услуг. В рамках данной методологии третьими сторонами могут считаться правительственные организации, суды или другие лица (компании, НПО, частные лица).

**Управленческое звено** — комитет, программа, команда или уполномоченное лицо, не являющееся частью высшего руководства компании.

**Уполномоченное лицо** — старший сотрудник, несущий ответственность за определенные действия компании и связанные с ними риски, в данном случае в сфере приватности и свободы самовыражения.

**Устройство / карманное устройство / мобильное устройство** — физический предмет (смартфон или телефон), используемый для доступа к телекоммуникационным сетям и предназначенный для переноски пользователем и использования в различных местах.

**Уязвимость защиты** — уязвимое место, которое позволяет злоумышленнику ослабить информационную безопасность системы. Уязвимость представляет собой совокупность трех параметров: восприимчивость или изъян системы, наличие у злоумышленника доступа к изъяну и способность злоумышленника воспользоваться данным изъяном.

**Флаг, созданный человеком** — флаг, оставленный человеком (пользователем, сотрудником или подрядчиком компании, работником органов власти, а также сотрудником или представителем частной организации). Также см. автоматический флаг.

**Цифровые платформы**. В методологии RDR цифровые платформы относятся к группе Индекса RDR, включающей в себя компании с экосистемами мобильной связи и Интернета, а также компании, управляющие услугами электронной коммерции и экосистемами персональных цифровых помощников.

**Частные запросы** — запросы, выдвигаемые в рамках частного, а не судебного или правительственного процесса. Частные запросы на ограничение контента или учетных записей могут исходить от неправительственных саморегулирующихся организаций (например, Internet Watch Foundation) или поступать в соответствии с системой уведомлений и запретов (например, Законом США об авторском праве в цифровую эпоху). Более подробную информацию об уведомительном и запретительном порядке, а также конкретно об упомянутом законе см. в книге «Содействие свободе в Интернете: Роль интернет-посредников», ЮНЕСКО, стр. 40-52 http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.http://unesdoc.unesco.org/images/0023/002311/231162e.pdf [анг].

Частные запросы на получение пользовательских данных часто носят неофициальный характер и не предполагают какого-либо формального юридического процесса. По данным Фонда Викимедиа, публикующего отчеты о прозрачности [анг] с данными о количестве полученных запросов такого рода, частные запросы на предоставление сведений о пользователях касаются, например, случаев, когда какая-либо компания направляет письмо или обращение по электронной почте с просьбой предоставить «непубличную информацию» об одном из пользователей. Информация может включать IP-адрес или адрес электронной почты пользователя.

**Четко раскрывает** — компания представляет или разъясняет свою политику или практическую деятельность в общедоступных материалах таким образом, чтобы пользователям было легко ее найти и понять.

**Шейпинг трафика** — регулирование потока сетевого трафика. Сюда может быть включено обусловленное замедление определенных типов трафика. Формирование трафика может использоваться в законных целях управления сетью (например, приоритет трафика VoIP перед обычным веб-трафиком для облегчения общения в реальном времени) или по причинам, противоречащим принципам сетевого

нейтралитета (например, намеренное замедление видеотрафика, чтобы отучить пользователей от использования приложений с высокой пропускной способностью).

**Шифрование** — позволяет скрыть содержимое переписки или файлов таким образом, чтобы его мог просмотреть только предполагаемый получатель. В процессе используется алгоритм для преобразования сообщения (открытого текста) в закодированный формат (шифротекст), так что сообщение выглядит как случайный набор символов для того, кто на него смотрит. Только обладатель соответствующего ключа шифрования может расшифровать сообщение, превратив шифрованный текст обратно в открытый. Данные могут быть зашифрованы как при хранении, так и при передаче.

Например, пользователи могут зашифровать данные на своем жестком диске таким образом, что только пользователь с ключом шифрования сможет расшифровать содержимое диска. Помимо этого, пользователи могут отправить зашифрованное сообщение электронной почты, в результате которого никто не сможет ознакомиться с содержимым письма, пока оно будет передаваться по сети до адресата. При шифровании в процессе передачи данных (например, когда веб-сайт использует HTTPS) связь между пользователем и веб-сайтом шифруется, так что сторонние лица, например, интернет-провайдер пользователя, могут просмотреть только первое посещение веб-сайта, но не информацию, передаваемую пользователем на этом сайте, или вложенные страницы, которые посещает пользователь.См: http://www.explainthatstuff.com/encryption.html [анг].

**Экосистема персонального цифрового помощника** — установленный на цифровых устройствах интерфейс с искусственным интеллектом, который может взаимодействовать с пользователями посредством текста или голоса для обеспечения доступа к информации в Интернете и выполнения определенных задач с использованием предоставленных пользователями личных данных. Пользователи могут взаимодействовать с экосистемами с помощью навыков (голосовых приложений), которые предоставляются либо сторонними разработчиками, либо самой экосистемой персонального цифрового помощника.

**Явно** — компания особо подчеркивает свою поддержку принципам свободы высказываний и неприкосновенности частной жизни.

Ranking Digital Rights

**Этот перевод методологии RDR 2020 был завершен в сентябре 2022 года.**