Правила программы для разработчиков

(дата вступления в силу: 1 января 2026 г., если не было указано иное)

Создадим самый надежный магазин приложений вместе

Ваши идеи и ответственность – залог нашего общего успеха. Правила программы для разработчиков и Соглашение о распространении программных продуктов помогают нам создавать самые инновационные и надежные приложения более чем для миллиарда пользователей Google Play. Рекомендуем ознакомиться с правилами ниже.

Запрещенный контент

Google Play используют люди со всего мира. Прежде чем опубликовать приложение, убедитесь, что оно соответствует требованиям нашего сервиса и законам страны, в которой вы его распространяете.

Нарушение прав ребенка

Мы немедленно удаляем из Google Play приложения, в которых пользователям разрешается создавать, загружать или распространять контент, связанный с эксплуатацией детей или жестоким обращением с ними (включая любые материалы, демонстрирующие несовершеннолетних в сексуальном контексте). Чтобы сообщить о таком контенте в продукте Google, нажмите **Пожаловаться** . Если вы обнаружите подобные материалы на других ресурсах в интернете, обратитесь напрямую в местную правозащитную организацию .

Мы не допускаем использование приложений с целью подвергнуть ребенка опасности. В частности, запрещена пропаганда эксплуататорского поведения, включая:

- недопустимые действия в отношении детей (например, ласки или ощупывание);
- совращение несовершеннолетних, например знакомство и общение с ребенком в интернете с целью совершения действий сексуального характера (онлайн или офлайн) и/или обмена с ним изображениями сексуального характера;
- сексуализация несовершеннолетних, например материалы, демонстрирующие, провоцирующие или поощряющие сексуальное насилие над детьми, или изображение детей таким образом, который может повлечь за собой их сексуальную эксплуатацию;
- шантаж разоблачениями половой жизни (например, угрозы или шантаж ребенка на основе реального или мнимого доступа к его интимным фотографиям);
- торговля детьми (например, приглашение и вовлечение ребенка в деятельность, ведущую к его дальнейшей коммерческой сексуальной эксплуатации).

Мы примем все необходимые меры вплоть до обращения в Национальный центр по борьбе с эксплуатацией и похищением детей (NCMEC), если нам станет известно о контенте с изображением несовершеннолетних в сексуальном контексте. Если вы считаете, что ребенок в опасности или ему угрожает сексуальное насилие или похищение, незамедлительно обратитесь в местные правоохранительные органы и свяжитесь с организацией по защите прав детей .

Кроме того, запрещены приложения, предназначенные для детей, но содержащие материалы для взрослых, в том числе:

- приложения со сценами насилия, изображениями крови и увечий;
- приложения, которые демонстрируют или поощряют опасные или причиняющие вред действия.

Запрещены приложения, формирующие негативное восприятие себя и собственного тела, например те, которые изображают в развлекательных целях пластическую хирургию, потерю веса и другие косметические корректировки внешнего вида.

Правила в отношении стандартов безопасности детей

Согласно требованиям Google Play приложения для знакомств и общения должны соответствовать правилам в отношении стандартов безопасности детей.

Требования к этим приложениям:

- **Опубликованные стандарты.** Необходимо разместить явный запрет на использование приложения в связи с сексуальным насилием над детьми и эксплуатацией детей. Его можно опубликовать в общедоступных условиях использования, правилах сообщества или других правилах для пользователей.
- **Сбор отзывов в приложении.** Вам нужно подтвердить, что в приложении у пользователей есть возможность отправлять отзывы, жалобы и вопросы.
- **Борьба с контентом, представляющим несовершеннолетних в сексуальном контексте.** Вы должны подтвердить, что при обнаружении в приложении подобных материалов будут приняты надлежащие меры (включая, удаление такого контента) в соответствии с опубликованными вами стандартами и применимым законодательством.
- **Соблюдение законов в отношении безопасности детей.** Вы должны подтвердить, что приложение соответствует действующему законодательству в отношении безопасности детей, в том числе позволяет отправлять жалобы на контент, представляющий несовершеннолетних в сексуальном контексте, в Национальный центр США по проблемам пропавших без вести и подвергающихся эксплуатации детей или похожую местную организация.
- **Информация о контактном лице по вопросам безопасности детей.** Google Play может присылать уведомления о том, что в вашем приложении или на вашей платформе обнаружен контент, связанный с сексуальным насилием над детьми и эксплуатацией детей. В приложении нужно указать, кто будет получать такие сообщения. Этот представитель должен знать, как вы проверяете материалы и что делаете в случае нарушений, и при необходимости принимать меры.

Вы можете узнать больше о перечисленных требованиях и их соблюдении.

Неприемлемый контент

Мы стремимся к тому, чтобы в Google Play было безопасно и комфортно всем пользователям. Ниже перечислены виды контента, который считается неподобающим и может причинить людям вред.

Контент сексуального характера и непристойная лексика

Запрещено публиковать приложения, содержащие или продвигающие материалы непристойного или сексуального характера (например, порнографию) и любой контент или услуги, предназначенные для сексуального удовлетворения. Кроме того, запрещены приложения и контент, в которых, по всей видимости, рекламируются или предлагаются сексуальные услуги, предоставляемые за вознаграждение. Также недопустимы приложения, которые содержат или продвигают контент, связанный с эксплуататорским сексуальным поведением, или распространяют материалы сексуального характера без согласия присутствующих в них лиц. Мы можем сделать исключение для содержащего наготу контента, если он в основном имеет образовательные, художественные, документальные или научные цели и не предназначен вызывать сексуальное возбуждение.

В приложениях с каталогами книг и фильмов различной тематики разрешается распространять книги (в том числе электронные издания и аудиокниги) и видео с контентом сексуального характера, если соблюдаются следующие условия:

- Книги и фильмы с контентом сексуального характера составляют малую долю от общего числа материалов, представленных в каталоге.
- В приложении нет активного продвижения фильмов или книг с контентом сексуального характера. Такие произведения могут появляться в рекомендациях на основе истории действий пользователя или во время рекламных акций.
- В приложении не распространяются книги или фильмы, в которых есть контент, создающий угрозу для детей, порнография или другие материалы сексуального характера, запрещенные действующим законодательством.
- Приложение защищает несовершеннолетних, ограничивая им доступ к книгам и фильмам с контентом сексуального характера.

Если приложение содержит материалы, которые не отвечают указанным здесь правилам, но считаются уместными в определенном регионе, оно может быть доступно в этом регионе, но не в других.

Вот примеры наиболее распространенных нарушений:

- Изображения, на которых присутствуют: обнаженные люди в сексуальном контексте и/или одетые неподобающе для появления на публике; непристойные позы, причем люди, их принимающие, почти или полностью раздеты либо их изображение размыто.
- Изображения, анимации и иллюстрации, содержащие сексуальные сцены и вызывающие позы или представляющие отдельные части тела в сексуальном контексте.
- Контент, который содержит изображение секс-игрушек или фетишей, является руководством по сексу или связан с незаконными сексуальными практиками.
- Контент, содержащий непристойную лексику, в том числе оскорбительные выражения, откровенные тексты и ключевые слова, связанные с сексом или темами для взрослых. Подобный контент также запрещен на страницах приложений в Google Play.
- Контент, описывающий, изображающий или поощряющий зоофилию.
- Приложения, продвигающие сексуальные развлечения, эскорт или другие формы сексуальных услуг, которые предоставляются за вознаграждение, в том числе сервисы, способствующие знакомствам или договоренностям о свиданиях, где один из участников предлагает другому деньги, подарки или финансовую поддержку.
- Приложения, в которых людей унижают или рассматривают как сексуальный объект. Например, сюда относятся утверждения, что приложение может виртуально раздевать людей или показывать то, что скрыто под одеждой (даже в качестве шуток и розыгрышей).
- Контент или действия, связанные с угрозами или эксплуатацией сексуального характера, включая фотосъемку без разрешения, запись видео и фотографирование скрытой камерой, изображения сексуального характера, созданные без разрешения в виде дипфейка или с помощью аналогичных технологий, а также оскорбительные материалы.

Дискриминационные высказывания

Запрещено публиковать приложения, пропагандирующие насилие или разжигающие ненависть к каким-либо лицам и социальным группам на почве расовой, этнической или национальной принадлежности, вероисповедания, инвалидности, возраста, статуса ветерана, сексуальной ориентации, пола, гендерной идентичности, касты, иммиграционного статуса и других признаков, связанных с систематической дискриминацией или маргинализацией.

Приложения, содержащие образовательные, художественные, документальные и научные материалы на тему нацизма, могут быть заблокированы в некоторых странах в соответствии с действующим законодательством.

Вот примеры наиболее распространенных нарушений:

- Контент или утверждения, призванные убедить в том, что определенная группа людей якобы неполноценна, ненормальна или заслуживает ненависти.

- Приложения, содержащие дискриминационные заявления, стереотипы или теории о том, что определенной группе людей якобы присущи негативные характеристики (например, жадность или безнравственность). Приложения, в которых явно или неявно утверждается, что некая группа людей представляет собой угрозу.
- Материалы или высказывания, созданные для того, чтобы убедить других в том, что людей можно ненавидеть или подвергать дискриминации на основании принадлежности к определенной группе.
- Материалы, которые продвигают поведение, атрибутику, флаги, символы или знаки отличия, связанные с группами, пропагандирующими ненависть.

Насилие

Запрещено публиковать приложения, которые изображают опасные действия или неоправданное насилие, а также способствуют им. Приложения, изображающие вымышленное насилие в контексте игры, как правило, разрешены. Например, в играх об охоте или рыбалке, а также построенных на сюжетах мультфильмов.

Вот примеры наиболее распространенных нарушений:

- Реалистичные изображения или подробные описания насильственных действий по отношению к человеку или животному.
- Приложения, пропагандирующие самоубийство, причинение себе вреда, нарушение пищевого поведения, игры с асфиксией и другие действия, которые могут привести к серьезным травмам или смерти.

Насильственный экстремизм

Мы не позволяем террористическим или другим опасным организациям или движениям, которые взяли на себя ответственность за акты насилия в отношении гражданских лиц, участвовали в них или готовились к ним, публиковать приложения в Google Play для любых целей, включая вербовку.

Запрещены приложения, в которых содержится контент, связанный с насильственным экстремизмом, а также материалы, касающиеся планирования, подготовки или поощрения насилия в отношении гражданских лиц, например пропагандирующие террористическую деятельность, призывающие к насилию и прославляющие теракты. Если такой контент содержится в ваших образовательных, документальных, научных или художественных материалах, сопроводите его необходимыми пояснениями.

Трагические события

Запрещается публиковать приложения, которые спекулируют на событиях, требующих деликатного отношения и имеющих существенное социальное, культурное или политическое влияние (гражданские чрезвычайные ситуации, природные катаклизмы, чрезвычайные ситуации в сфере здравоохранения, конфликты, смерти и другие трагические события), или выражают крайнее пренебрежение ими. Приложения, содержащие материалы о событии, требующем деликатного отношения, могут быть разрешены. Это касается случаев, когда контент имеет образовательную, документальную, научную или художественную ценность либо создан, чтобы предупредить или проинформировать пользователей об этом событии.

Вот примеры наиболее распространенных нарушений:

- Бестактность по отношению к смерти реального человека или группы людей, наступившей в результате естественных причин, самоубийства, передозировки и т. д.
- Отрицание известного трагического события, подтвержденного документально.
- Извлечение выгоды из события, требующего деликатного отношения, без оказания явной помощи пострадавшим.

Издевательства и угрозы

Запрещено публиковать приложения, содержащие угрозы, издевательства и домогательства, а также способствующие совершению таких действий.

Вот примеры наиболее распространенных нарушений:

- Издевательства над жертвами международных или религиозных конфликтов.
- Материалы, направленные на эксплуатацию других людей, например на вымогательство или шантаж.
- Размещение материалов с целью публично кого-то унизить.
- Нападки на лиц, пострадавших в результате трагического события, или на их родственников и друзей.

Опасные товары

Запрещается публиковать приложения, с помощью которых можно приобрести взрывчатые вещества, огнестрельное оружие, патроны, а также некоторые детали для огнестрельного оружия.

- Запрещены детали и приспособления, которые позволяют имитировать автоматический огонь или предназначены для переделки оружия в автоматическое, в том числе подвижные ложи, автоматические спусковые устройства, наборы для переоборудования оружия, а также магазины и ленты, содержащие более 30 патронов.

Запрещено публиковать приложения, содержащие инструкции по производству взрывчатых веществ, огнестрельного и другого оружия, патронов, а также запрещенных деталей для огнестрельного оружия. Это относится в том числе к инструкциям по имитации автоматического огня или переделке огнестрельного оружия в автоматическое.

Марихуана

Запрещено публиковать приложения, с помощью которых можно приобрести марихуану или продукты с ней (независимо от того, насколько такие покупки законны).

Вот примеры наиболее распространенных нарушений:

- Приложения, в которых пользователи могут заказать марихуану с помощью встроенной корзины.
- Сервисы, которые помогают пользователям организовать доставку марихуаны.
- Сервисы, которые облегчают приобретение продуктов, содержащих тетрагидроканнабинол, в том числе масел на основе каннабидиола.

Табачные изделия и алкоголь

Запрещено публиковать приложения, с помощью которых можно покупать табачные изделия и содержащие никотин товары, в том числе электронные сигареты, вейпы и сосательный табак, а также приложения, поощряющие незаконное или недопустимое потребление алкоголя, табака или никотина.

Дополнительная информация

- Запрещается изображать то, как несовершеннолетние употребляют или приобретают алкогольные напитки и табачные изделия. Также не разрешено поощрять их продажу детям и побуждать несовершеннолетних потреблять такие продукты.
- Недопустимы материалы, подразумевающие, что употребление табака может повысить интеллект, статус в обществе или улучшить профессиональное положение, сексуальную жизнь или физическую форму.

- Не разрешается создавать положительный образ чрезмерного употребления алкоголя, в том числе запоев и соревнований по распитию спиртных напитков.
- Запрещается рекламировать, продвигать и явно демонстрировать табачные изделия. Это также относится к связанным с ними баннерам, категориям товаров и ссылкам на сайты, где продается табак.
- Мы можем разрешить ограниченную продажу табачных изделий в приложениях для доставки еды/продуктов в некоторых регионах при условии соблюдения защитных мер по проверке возраста (например, проверки удостоверения личности при доставке).
- Мы можем разрешить продажу товаров, рекламируемых в качестве помощи для избавления от никотиновой зависимости, при условии соблюдения защитных мер по проверке возраста.

Финансовые услуги

Запрещено публиковать приложения, предоставляющие пользователям доступ к вводящим в заблуждение или вредоносным финансовым продуктам и услугам.

Финансовыми считаются все продукты и услуги, связанные с управлением финансами, инвестициями и криптовалютами, в том числе персональные консультации.

Если ваше приложение предлагает или рекламирует финансовые продукты и услуги, оно должно соответствовать требованиям государственного и муниципального законодательства во всех странах и регионах, для которых оно предназначено,—например, содержать информацию, особо оговоренную в местных законах.

Разработчикам приложений, в которых есть финансовые функции, нужно заполнить специальную декларацию в Play Console.

Бинарные опционы

Запрещено публиковать приложения, позволяющие пользователям торговать бинарными опционами.

Кредиты

Согласно нашим правилам, к потребительским кредитам относятся ссуды, единовременно выдаваемые физическим лицом или организацией отдельному клиенту не для приобретения основных средств или оплаты образования. Чтобы потребители могли принять взвешенное решение, необходимо предоставить им сведения о качестве, характеристиках, комиссии, графиках погашения, рисках и преимуществах кредитных предложений.

- Примеры: потребительские кредиты, кредиты наличными, займы между физическими лицами, кредиты под залог автомобиля.
- В эту категорию не входят: ипотека, кредиты на покупку автомобилей и возобновляемые кредиты, в том числе карты и персональные кредитные счета.

К займам в счет заработной платы относятся финансовые услуги, с помощью которых физическое лицо может получить часть заработанных им (но ещё не выплаченных работодателем) средств. Займы такого типа имеют следующие отличия от классических кредитов:

- Механизм погашения. Займ возвращается автоматически: сумма вычитается из заработной платы или выплачивается через автоплатеж, подключенный к банковскому счету пользователя. При неуспешном автоплатеже дополнительные проценты, пени или комиссии не взимаются.
- Ограничение на основе дохода. Максимально доступный займ строго ограничен суммой, уже заработанной пользователем в течение текущего платежного периода, поэтому не может выдаваться в счет будущих доходов.

- Структура комиссий. К займам в счет заработной платы не применяются процентные ставки. За использование таких услуг сервис взимает небольшую комиссию: фиксированную или в виде процентной доли от транзакции. Обоснованной считается минимальная и прозрачная комиссия, отражающая реальную стоимость предоставления услуги и не обременяющая пользователя. Например, комиссия может составлять 1–5 долларов США за транзакцию или 1–5 % от выданного займа.
- Отсутствие записей в кредитной истории. Обычно сервисы, предлагающие займы в счет заработной платы, не передают сведения о транзакциях в кредитные бюро, поэтому услуги такого типа не влияют на кредитный рейтинг и не способствуют росту долгосрочных долгов пользователя.

Если вы предлагаете потребительские кредиты, в том числе выдаете их напрямую, занимаетесь привлечением потенциальных клиентов или помогаете потребителям связываться со сторонними кредиторами, выберите в Play Console категорию "Финансы" для приложения и обязательно укажите следующую информацию в его метаданных:

- минимальный и максимальный период погашения долга;
- максимальную годовую процентную ставку, в которую обычно входит ставка по кредиту, а также комиссии и прочие расходы за год, или другую аналогичную ставку, отвечающую требованиям местного законодательства;
- показательный пример расчета общей стоимости займа, включая основную сумму долга и все действующие комиссии;
- политику конфиденциальности, в которой подробно описано, как и для чего приложение собирает и использует личные и конфиденциальные пользовательские данные, а также получает и предоставляет к ним доступ в соответствии с ограничениями, указанными в этом правиле.

Запрещено публиковать приложения, предлагающие потребительские кредиты, которые необходимо полностью погасить в течение 60 дней после выдачи или раньше (краткосрочные потребительские кредиты).

Если вы предлагаете займы в счет заработной платы, в том числе выдаете их напрямую, занимаетесь привлечением потенциальных клиентов или помогаете потребителям связываться со сторонними кредиторами, выберите в Play Console категорию "Финансы" для приложения и обязательно укажите следующую информацию в его метаданных:

- условия погашения долга;
- все комиссии, в том числе за использование услуги, за транзакции, а также любые другие, действующие при выдаче займа;
- показательный пример расчета общей стоимости займа, включая все комиссии;
- политику конфиденциальности, в которой подробно описано, как и для чего приложение собирает и использует личные и конфиденциальные пользовательские данные, а также получает и предоставляет к ним доступ в соответствии с ограничениями, указанными в этом правиле.

У нас должна быть возможность установить связь между вашим аккаунтом разработчика и любыми лицензиями и документами, которые вы отправляете нам для подтверждения права предоставлять потребительские кредиты. Мы также можем запросить дополнительные сведения или документы, чтобы убедиться, что вы соблюдаете местное действующее законодательство.

Приложения, в которых предлагаются потребительские кредиты или основным назначением которых является помощь в получении таких кредитов (например, поиск клиентов или посредников), приложения, где можно открывать кредитные линии, вспомогательные приложения для желающих взять кредит (например, кредитные калькуляторы, справочники по кредитным условиям и т. д.), а также приложения, в которых предоставляются займы в счет заработной платы, не должны иметь доступ к конфиденциальной информации, в том числе фотографиям и контактам. Запрещается использовать следующие разрешения:

- Read_external_storage;
- Read_media_images;
- Read_contacts;
- Access_fine_location;
- Read_phone_numbers;
- Read_media_videos;
- Query_all_packages;
- Write_external_storage.

К приложениям, в которых используется конфиденциальная информация или API с доступом к таким данным, применяются дополнительные требования и ограничения. Дополнительную информацию вы найдете в правилах использования разрешений.

Потребительские кредиты с высокой годовой процентной ставкой

В США запрещены приложения, предлагающие потребительские кредиты с годовой процентной ставкой от 36 %. Публикуемые в США приложения, предлагающие потребительские кредиты, должны содержать информацию о максимальной годовой процентной ставке, рассчитанной в соответствии с законом "О справедливом кредитовании" (TILA) .

Эти правила относятся к приложениям, которые предлагают кредиты напрямую, ищут потенциальных клиентов или помогают потребителям связываться со сторонними кредиторами.

Требования в отдельных странах

Приложения, предлагающие потребительские кредиты пользователям из указанных ниже стран, должны отвечать дополнительным требованиям. Кроме того, их разработчики должны заполнить в Play Console декларацию финансовых функций и отправить нам указанные в ней документы. Для приложений, выдающих займы в счет заработной платы, эти требования действуют в мере, применимой в соответствующих юрисдикциях. Вы обязаны по запросу Google Play предоставить дополнительные сведения или документы, подтверждающие соответствие действующим нормативным и лицензионным требованиям.

1. **Индия**
   - Если у вас есть лицензия Резервного банка Индии на выдачу потребительских кредитов, отправьте нам для проверки ее копию.
   - Если вы не участвуете в кредитовании напрямую и только предоставляете платформу, которая упрощает процесс выдачи кредитов зарегистрированными небанковскими кредитными организациями (НБФО) или банками, укажите это в декларации.
     - Наименования всех зарегистрированных НБФО и банков должны быть перечислены в описании приложения, и эта информация должна быть хорошо заметна.
2. **Индонезия**
   - Если ваше приложение связано с оказанием услуг цифрового кредитования в соответствии с Положением OJK № 77/POJK.01/2016 (может время от времени изменяться), вы обязаны предоставить нам для проверки копию действующей лицензии.
3. **Филиппины**
   - Все финансовые и кредитные компании, предлагающие кредиты через платформы онлайн-кредитования, должны получить регистрационный номер SEC (SEC Registration Number) и номер сертификата полномочий (Certificate of Authority Number) от Комиссии Филиппин по ценным бумагам и биржам (PSEC).
     - В описании приложения также необходимо указать название компании/корпорации, регистрационный номер PSEC и номер сертификата полномочий на управление финансовой или кредитной организацией (Certificate of Authority to Operate a Financing/Lending Company).

- Приложения, связанные с основанной на кредитовании краудфандинговой деятельностью, такой как P2P-кредитование, или другой подобной деятельности, указанной в филиппинских Положениях о краудфандинге (CF Rules), должны обрабатывать транзакции через краудфандинговых посредников, зарегистрированных Комиссией Филиппин по ценным бумагам и биржам.

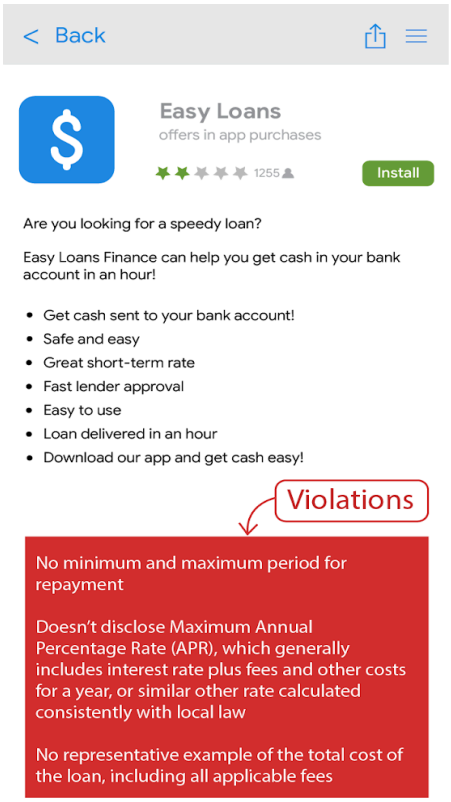
4. **Нигерия**
   - Цифровые кредиторы (ЦК) должны заполнить форму LIMITED INTERIM REGULATORY/REGISTRATION FRAMEWORK AND GUIDELINES FOR DIGITAL LENDING образца 2022 года (может время от времени изменяться), которая утверждена Федеральной антимонопольной комиссией по защите прав потребителей (FCCPC) Нигерии, и придерживаться указанных в форме положений. Также необходимо получить верифицируемое письмо-подтверждение от FCCPC.
   - Агрегаторы кредитных предложений обязаны предоставлять документы, подтверждающие право оказывать услуги цифрового кредитования, а также контактную информацию всех ЦК, с которыми они сотрудничают.

5. **Кения**
   - Цифровые кредиторы (ЦК) должны пройти процедуру регистрации ЦК и получить лицензию от Центрального банка Кении (ЦБК). Вместе с декларацией вам необходимо предоставить копию своей лицензии от ЦБК.
   - Если вы не участвуете в кредитовании напрямую и только предоставляете платформу, которая упрощает процесс выдачи кредитов зарегистрированными ЦК, укажите это в декларации и предоставьте копии лицензий ЦБК для своих партнеров.
   - Сейчас мы принимаем декларации и лицензии только от лиц, которые перечислены в Реестре цифровых кредиторов (Directory of Digital Credit Providers), опубликованном на официальном сайте ЦБК.

6. **Пакистан**
   - Любая небанковская кредитная организация (НБФО) может опубликовать только одно приложение для цифрового кредитования. Если вы попытаетесь разместить несколько таких приложений, ваш аккаунт разработчика и все связанные аккаунты могут быть заблокированы.
   - Чтобы оказывать услуги цифрового кредитования в Пакистане или помогать в их получении, нужно отправить выданное Комиссией по ценным бумагам и биржам Пакистана (SECP) свидетельство, подтверждающее право на такую деятельность. Кроме того, запрещено публиковать приложения, в которых предлагаются краткосрочные потребительские кредиты, однако в редких случаях мы можем делать исключения на территории Пакистана в соответствии с действующим законодательством.

7. **Таиланд**
   - Разработчикам приложений, предлагающих потребительские кредиты в Таиланде с процентной ставкой 15 % и выше, нужно получить лицензию от Банка Таиланда или Министерства финансов. Они также должны предоставить документы, подтверждающие, что с помощью приложения можно получать потребительские кредиты в этой стране или подавать заявку на них. В частности, необходимо отправить:
     - Копию лицензии на деятельность в качестве нанофинансовой организации или поставщика потребительских кредитов. Документ должен быть выдан Банком Таиланда.
     - Копия лицензии на деятельность в качестве пикофинансовой организации. Документ должен быть выдан Министерством финансов.

Вот пример распространенного нарушения:



Азартные игры, игры и соревнования с реальными денежными призами

Приложения и рекламные объявления, связанные с азартными играми на реальные деньги, а также программы лояльности в игровой форме и приложения для коротких фэнтези-турниров разрешены при условии, что они соответствуют определенным требованиям.

Приложения для азартных игр

Допускаются приложения, которые позволяют или помогают участвовать в азартных онлайн-играх в определенных странах, если соблюдены все ограничения и правила Google Play, а разработчик подал заявку на распространение в Google Play приложений для азартных игр и получил разрешение. При этом разработчик является одобренным государственным оператором и/или зарегистрирован в местном ведомстве, отвечающем за игорную деятельность, и предоставил действующую лицензию для осуществления в стране той игорной деятельности, которую он предлагает.

Мы допускаем только те лицензированные или разрешенные приложения, которые предлагают следующие виды азартных онлайн-игр:

- онлайн-казино;
- ставки на результаты спортивных соревнований;
- скачки (где регулирование и лицензирование осуществляются отдельно от ставок на спорт);
- лотереи;
- короткие фэнтези-турниры.

Разрешенные приложения должны соответствовать следующим требованиям:

- Разработчик подал заявку и получил разрешение на распространение приложения через Google Play.

- Приложение не нарушает действующие законы и отраслевые стандарты страны, в которой оно будет распространяться.
- У разработчика есть действующая лицензия на ведение игорной деятельности для всех стран или штатов/территорий, где распространяется приложение.
- Разработчик не предлагает те виды азартных игр, которые выходят за рамки его лицензии.
- Приложение недоступно для несовершеннолетних.
- Приложение недоступно в странах, штатах/регионах или географических районах, на которые не распространяется лицензия разработчика.
- Приложение распространяется в Google Play бесплатно и НЕ использует функцию оплаты контента через Google Play.
- Приложение можно бесплатно скачать из Google Play.
- Приложению присвоено возрастное ограничение "Только для взрослых" или эквивалентное согласно рейтингу IARC.
- В приложении и на его странице в Google Play есть описание принципов ответственной игры.

Прочие приложения, связанные с азартными играми на реальные деньги, конкурсами и турнирами

Во всех других приложениях, которые не соответствуют вышеперечисленным требованиям к приложениям для азартных игр и которые не указаны в разделе "Другие пилотные игровые проекты с реальной валютой" ниже, запрещается публиковать контент или сервисы, которые позволяют или помогают заключать пари, делать ставки или иным образом использовать реальные деньги (в том числе совершать покупки в приложении) с целью получить приз, который имеет реальную денежную стоимость. Это касается в том числе онлайн-казино, спортивных тотализаторов, лотерей и игр, в которых принимаются деньги, а выигрышем являются денежные и другие ценные призы (кроме программ, соответствующих описанным ниже требованиям к программам лояльности в игровой форме).

Примеры нарушений

- Игры, в которых принимаются деньги в обмен на возможность выиграть денежный или иной материальный приз.
- Приложения, которые содержат элементы навигации или функции (пункты меню, вкладки, кнопки, компоненты WebView и т. д.) с призывом сделать ставку, заключить пари или принять участие в играх, конкурсах или соревнованиях с реальными денежными призами, например "Сделайте ставку!", "Зарегистрируйтесь!" или "Победите в соревновании!".
- Приложения, которые принимают ставки, используют внутреннюю валюту, выплачивают выигрыши или берут залог в обмен на возможность выиграть денежный или иной материальный приз.

Другие пилотные игровые проекты с реальной валютой

Периодически мы можем реализовывать в некоторых регионах ограниченные по времени пилотные проекты для определенных типов игр на реальные деньги. Подробную информацию вы найдете в этой статье Справочного центра. Пилотный проект по распространению приложений для онлайн-управления кран-машиной, который мы проводили в Японии, завершился 11 июля 2023 года. С 12 июля 2023 года в Google Play разрешено публиковать такие приложения по всему миру при условии, что соблюдены действующие законы и определенные требования.

Программы лояльности в игровой форме

Программы лояльности, которые поощряют пользователей материальными или денежными призами, разрешены, если они допускаются законом и не требуют получения дополнительной лицензии для азартных игр. Программы лояльности должны соответствовать перечисленным ниже требованиям Google Play.

Все приложения (игровые и неигровые)

- Преимущества, бонусы или вознаграждения, предоставляемые в рамках программы лояльности, должны быть явно дополнительными и второстепенными по отношению к любой квалифицированной денежной транзакции в приложении (где квалифицированная денежная транзакция – отдельная транзакция с целью предоставления товаров или услуг, не связанных с программой лояльности). Преимущества, бонусы или вознаграждения не могут быть предметом покупки или иметь отношение к какому-либо способу обмена. В противном случае это будет считаться нарушением Правил в отношении азартных игр, игр и соревнований с реальными денежными призами.
  - Например, ни одна часть квалифицированной денежной транзакции не может служить платой или ставкой для участия в программе лояльности. Также квалифицированная денежная транзакция не должна приводить к покупке товаров или услуг по повышенной цене.

Игровые приложения

- Бонусные баллы или вознаграждения с бонусами, преимуществами и наградами, связанными с квалифицированной денежной транзакцией, могут начисляться и использоваться только на основе фиксированной пропорции при условии, что она четко обозначена в приложении и общедоступных официальных правилах программы. Преимущества или выкупная стоимость **не могут** быть получены, начислены или приумножены в зависимости от успеха пользователя в игре или случайного результата.

Неигровые приложения

- Бонусные баллы или вознаграждения могут начисляться по результатам конкурса или случайного результата, если они соответствуют требованиям, указанным ниже. Для программ лояльности с преимуществами, бонусами или наградами, связанными с квалифицированной денежной транзакцией, необходимо:
  - разместить в приложении официальные правила программы;
  - если система вознаграждения меняется или основана на случайном или вероятностном выборе, в рамках официальных правил программы необходимо раскрыть: 1) вероятность – для любой системы вознаграждения, в которой для определения победителя используются фиксированные коэффициенты; 2) метод выбора (например, переменные, используемые для определения победителя) – для других подобных программ;
  - указать в официальных правилах программы с розыгрышами, лотереями или другими подобными промоакциями фиксированное число победителей, срок подачи заявок и дату вручения призов для каждой такой промоакции;
  - указать фиксированные коэффициенты начисления и погашения бонусных баллов или наград на видном месте в приложении, а также в официальных правилах программы.

Тип приложения с программой лояльности	**Игровая форма и меняющиеся вознаграждения**	**Награды на основе фиксированной пропорции**	**Условия использования программы лояльности**	**Указание доли вероятности или метода выбора в Условиях использования любой программы лояльности со случайным розыгрышем призов**
Игра	Запрещено	Разрешено	Обязательно	Неприменимо (в игровых приложениях для программ лояльности нельзя использовать элементы,

Тип приложения с программой лояльности	**Игровая форма и меняющиеся вознаграждения**	**Награды на основе фиксированной пропорции**	**Условия использования программы лояльности**	**Указание доли вероятности или метода выбора в Условиях использования любой программы лояльности со случайным розыгрышем призов**
				основанные на случайности)
Неигровое приложение	Разрешено	Разрешено	Обязательно	Обязательно

Приложения, распространяемые в Google Play, которые содержат рекламу азартных игр, а также игр, конкурсов и турниров на реальные деньги

Приложения с рекламой азартных игр, а также игр, конкурсов и соревнований с реальными денежными призами разрешены, если выполняются перечисленные ниже условия.

- Приложение, объявление и рекламодатель не нарушают законы и отраслевые стандарты страны, в которой объявление будет показываться.
- Объявление соответствует всем действующим местным требованиям к лицензированию продуктов и услуг, связанных с азартными играми.
- Приложение не показывает рекламу азартных игр лицам, не достигшим 18 лет.
- Приложение не входит в программу "Приложения для всей семьи".
- Лица, не достигшие 18 лет, не входят в целевую аудиторию приложения.
- Если рекламируются приложения для азартных игр (см. выше), на целевой странице объявления, в описании приложения в Google Play или в самом приложении должны содержаться четкие сведения о принципах ответственной игры.
- Приложение не является симулятором азартных игр (таких как казино или виртуальные игровые автоматы).
- Приложение не оказывает услуги, связанные с азартными играми, а также играми, лотереями и соревнованиями с реальными денежными призами или сопутствующими функциями (например, не помогает делать ставки, выводить выигрыши, отслеживать счет, котировки и результаты или управлять игровыми фондами).
- Приложение не продвигает азартные игры на реальные деньги и связанные с ними сервисы.

Реклама азартных игр, а также игр, лотерей и соревнований с реальными денежными призами допускается только в приложениях, соответствующих всем перечисленным выше требованиям,и в разрешенных приложениях для азартных игр (см. выше) или коротких фэнтези-турниров (см. ниже) при условии, что они соответствуют требованиям 1–6.

Примеры нарушений

- Приложение для несовершеннолетних, рекламирующее сервисы, связанные с азартными играми.
- Симулятор казино, который продвигает реальное казино или перенаправляет в него пользователей.
- Приложение для отслеживания шансов на победу в спортивных соревнованиях, содержащее ссылки на сайт, где принимаются ставки.
- Приложения, содержащие рекламу азартных игр, которая нарушает правила об объявлениях, вводящих в заблуждение, например рекламные объявления, которые выглядят как кнопки, значки или другие интерактивные элементы.

Приложения для коротких фэнтези-турниров

Приложения для коротких фэнтези-турниров, соответствующие требованиям действующего местного законодательства, разрешены, если выполняются перечисленные ниже условия.

- Приложение или 1) распространяется исключительно в США; или 2) соответствует требованиям к приложениям для азартных игр. Для распространения приложения за пределами США разработчик должен подать заявку, как указано выше.
- Разработчик подал заявку и получил разрешение на распространение приложения в Google Play.
- Приложение не нарушает законы и отраслевые стандарты стран, в которых оно распространяется.
- Возможность делать ставки или проводить денежные транзакции в приложении недоступна для несовершеннолетних.
- Приложение распространяется в Google Play бесплатно и НЕ использует функцию оплаты контента через Google Play.
- Приложение можно бесплатно скачать из Google Play.
- Приложению присвоено возрастное ограничение "Только для взрослых" или эквивалентное согласно рейтингу IARC.
- В приложении и на его странице в Google Play есть описание принципов ответственной игры.
- Приложение не нарушает действующие законы и отраслевые стандарты тех штатов или территорий США, где оно будет распространяться.
- У разработчика есть действующая лицензия на распространение приложения для каждого штата или территории США, где такая лицензия требуется.
- Если у разработчика нет лицензии на распространение приложения в каких-то штатах или на некоторых территориях США, то оно должно быть там недоступно.
- Приложение недоступно в тех штатах и на тех территориях США, где приложения для коротких фэнтези-турниров запрещены законом.

Незаконные действия

Запрещено публиковать приложения, которые способствуют совершению незаконных действий или поощряют их.

Вот примеры наиболее распространенных нарушений:

- Покупка и продажа запрещенных препаратов.
- Изображение того, как несовершеннолетние используют или приобретают наркотики, алкоголь и табачные изделия, а также поощрение этого.
- Инструкции по производству запрещенных препаратов, в том числе по выращиванию наркотических растений.

Контент, созданный пользователями

К этой категории относится контент, создаваемый пользователями, который виден или доступен нескольким пользователям приложения.

В содержащих такой контент приложениях, включая специальные браузеры или клиенты, перенаправляющие пользователей на платформу с таким контентом, должна быть реализована надежная, эффективная и стабильная система модерации пользовательского контента. Вот требования к такой системе:

- Перед тем как создавать или загружать материалы, пользователи должны принимать условия использования и/или правила для пользователей.

- Должны быть даны определения нежелательного контента и поведения (согласующиеся с Правилами программы для разработчиков приложений в Google Play). Условия использования или правила для пользователей должны запрещать нежелательный контент и поведение.
- Пользовательский контент должен модерироваться настолько, насколько это уместно для того типа материалов, которые размещаются в приложении. Помимо прочего, в приложении должна быть реализована система, позволяющая подавать жалобы и блокировать нежелательный контент и пользователей. При необходимости разработчик должен принимать меры против таких материалов и пользователей. Разные сценарии работы с контентом, созданным пользователям, могут требовать разных подходов к модерации. Например:
  - Если приложение позволяет идентифицировать определенную группу пользователей такими средствами, как верификация или офлайн-регистрация (например, приложения, предназначенные для учеников школы или сотрудников компании), то в нем должна быть реализована функция, позволяющая жаловаться на контент и пользователей.
  - Если пользователи в приложении могут взаимодействовать друг с другом один на один (например, переписываться напрямую, а также отмечать или упоминать кого-то в контенте или чате), то в нем должна быть функция блокировки пользователей.
  - Если приложение предоставляет доступ к общедоступным материалам, созданным пользователями (например, приложения для социальных сетей и ведения блогов), то в нем должна быть функциональность, позволяющая блокировать пользователей и жаловаться на них и контент.
  - В AR-приложениях модерация пользовательского контента (включая систему отправки жалоб в приложении) должна состоять в проверке как на нежелательный пользовательский контент (например, AR-изображения сексуального характера), так и на конфиденциальность местоположения, к которому привязана дополненная реальность (например, военные базы или частные владения, поскольку такая привязка может создавать проблемы для собственников).
- Должны быть приняты меры предосторожности для того, чтобы монетизация в приложении не способствовала нежелательному поведению пользователей.

Эпизодический встречающийся контент сексуального характера

Контент сексуального характера считается эпизодически встречающимся, если он появляется в приложении с созданным пользователями контентом, которое: 1) предоставляет доступ к материалам преимущественно несексуального характера; 2) не продвигает и не рекомендует контент сексуального характера. Контент сексуального характера, определяемый действующим законодательством как незаконный, а также контент, создающий угрозу для детей, не считается эпизодически встречающимся. Его размещение запрещено.

Эпизодически встречающийся контент сексуального характера допускается в приложениях с контентом, созданным пользователями, при соблюдении всех следующих условий:

- Такой контент по умолчанию скрыт фильтрами, для полного снятия которых требуется как минимум два действия. Например, он может быть скрыт за межстраничным объявлением или по умолчанию доступен только после отключения безопасного поиска.
- Доступ к приложению явным образом заблокирован для детей (о том, кто считается детьми, рассказывается в правилах программы "Приложения для всей семьи") при помощи систем проверки возраста, например нейтрального возрастного фильтра или других систем, определенных действующим законодательством.
- Вы предоставили исчерпывающие ответы в анкете для присвоения возрастного ограничения относительно контента, созданного пользователями, как этого требуют правила в отношении возрастных ограничений.

Мы удаляем из Google Play приложения, основное назначение которых заключается в публикации нежелательного контента, созданного пользователями. Так же мы поступаем с приложениями, в которых пользователи начинают размещать главным образом нежелательный контент или

которые становятся известны среди пользователей тем, что нежелательный контент в них не удаляется.

Вот примеры наиболее распространенных нарушений:

- Продвижение материалов сексуального характера, созданных пользователями, включая реализацию платных функций, которые способствуют распространению нежелательного контента.
- Приложения с контентом, созданным пользователями, где не обеспечена достаточная защита от угроз, домогательств или издевательств, особенно по отношению к несовершеннолетним.
- Записи, комментарии и фотографии в приложении, предназначенные для запугивания другого человека или призывающие к оскорблениям, вредоносным действиям и насмешкам по отношению к нему.
- Приложения, разработчики которых игнорируют жалобы пользователей на неприемлемый контент.

Контент и сервисы, связанные со здоровьем

Запрещено публиковать приложения, предоставляющие пользователям доступ к опасным контенту и сервисам, связанным со здоровьем.

Приложения, которые предлагают или рекламируют контент и сервисы, связанные со здоровьем, должны соответствовать требованиям действующего законодательства.

Приложения для здоровья и медицинские приложения

Если приложение содержит функции или сведения, связанные со здоровьем, или получает доступ к данным о здоровье для работы других функций, оно должно соответствовать текущим правилам для разработчиков приложений в Google Play, включая правила в отношении нарушения конфиденциальности, злоупотребления ресурсами устройства и мошенничества, а также перечисленным ниже требованиям.

- **Декларация в Play Console:**
  - Все разработчики должны заполнить декларацию на странице "Контент приложения" ("Правила > Контент приложения") в Play Console. Подробнее о том, как заполнять форму декларации приложений для здоровья...
- **Требования к политике конфиденциальности и раскрытию информации:**
  - Ссылка на политику конфиденциальности должна быть приведена в предназначенном для нее разделе Play Console и в самом приложении (допускается разместить текст правил). Убедитесь, что текст политики конфиденциальности (не в виде PDF-файла) доступен по активной общедоступной ссылке без ограничений по геозоне, не может быть изменен и соответствует информации из раздела безопасности данных.
  - В политике конфиденциальности и в сообщениях о раскрытии информации, размещенных в приложении, необходимо подробно объяснить, как оно собирает и использует личные и конфиденциальные пользовательские данные, а также получает и предоставляет к ним доступ. Это относится к любым сведениям, а не только к указанным в разделе безопасности данных. Если в приложении есть функции или данные, для доступа к которым нужны опасные или динамические разрешения , оно должно соответствовать всем действующим требованиям к раскрытию информации и получению разрешения на использование данных.
  - Нельзя запрашивать разрешения, от которых не зависит работа основных функций приложения для здоровья. Неиспользуемые разрешения нужно удалить. Список разрешений, связанных с данными деликатного характера о здоровье, приведен в разделе "Какие разрешения охватывают правила в отношении приложений для здоровья?" этой статьи Справочного центра.
  - Даже если основное назначение приложения не связано со здоровьем, но в нем есть касающиеся здоровья функции и доступ к данным о здоровье, на него распространяются

правила в отношении приложений для здоровья. Пользователям должна быть очевидна связь между основными функциями приложения и причинами, по которым собираются данные о здоровье. Например, приложению страховой компании может быть нужен доступ к медицинским данным для оформления полиса, а игре – к сведениям о физической активности для продвижения в игровом процессе. Это ограничение на использование данных должно быть отражено в политике конфиденциальности приложения.

- **Функции, связанные со здоровьем и медициной:**
  - Запрещены приложения, в которых связанные со здоровьем и медициной функции вводят в заблуждение или могут нанести вред.
  - Если приложения связываются с внешними устройствами или аппаратным обеспечением, например приборами для измерения уровня сахара в крови, для выполнения медицинских функций, то в описании приложений необходимо явным образом перечислить требования к этому оборудованию. Нельзя создавать у пользователей впечатление, что такие приложения могут работать независимо от необходимого внешнего аппаратного обеспечения.
  - Если приложения используют датчики устройства, например камеру, для выполнения функций, связанных со здоровьем, в описании приложений необходимо явным образом указать информацию о совместимости. Например, разработчики приложений, позволяющих измерять уровень кислорода в крови с помощью только датчиков устройства, должны перечислить модели, поддерживающие эту возможность.
  - Разработчики, у которых есть разрешение или одобрение регулирующих органов на квалификацию своих приложений как медицинских изделий, должны предоставить подтверждающие документы по запросу. Для приложений, которые не регулируются и не одобрены органом здравоохранения, требуется ясный отказ от обязательств с информацией о том, что они не являются медицинскими изделиями и не предназначены для диагностики, лечения и профилактики каких-либо заболеваний.
  - В приложениях также должны быть напоминания для пользователей о необходимости обращаться за консультациями, диагностикой и лечением к медицинским работникам.
- **Дополнительные требования:**
  Если ваше приложение для здоровья относится к одной из указанных ниже групп, вы должны выполнить действующие для него требования.
  - **Приложения для здоровья, связанные с государственными учреждениями.** Если вы получили от государственного учреждения или аккредитованной организации в сфере здравоохранения разрешение на разработку и распространение приложения в партнерстве с ними, вы должны предоставить нам подтверждающие документы через форму предварительного уведомления.
  - **Приложения для отслеживания контактов и состояния здоровья.** Если ваш продукт предназначен для отслеживания контактов с инфицированными и/или состояния здоровья, выберите в Play Console категорию "Профилактика болезней и общественное здравоохранение". Вам также нужно заполнить форму предварительного уведомления, упомянутую выше.
  - **Приложения для исследований с участием людей.** Приложения, в которых проводятся исследования в области здравоохранения с участием людей, должны соответствовать всем правилам и законам. Помимо прочего, это означает, что необходимо получать информированное согласие от совершеннолетних участников или от родителей или опекунов несовершеннолетних. Разработчикам таких приложений также следует получить одобрение на проведение исследований от институционального наблюдательного совета и/или аналогичного независимого комитета по этике, если для них не предусмотрено исключение. Свидетельство такого одобрения необходимо предоставить по запросу.

Подробную информацию о приложениях для здоровья и медицинских приложениях можно найти в этой статье Справочного центра.

Данные приложения "Здоровье и спорт"

Данные, доступ к которым осуществляется с помощью разрешений на доступ к приложению "Здоровье и спорт", считаются персональной и конфиденциальной пользовательской информацией. К ним применяются правила в отношении пользовательских данных и дополнительные требования .

Лекарства, отпускаемые по рецепту

Мы запрещаем публиковать приложения, предназначенные для продажи или покупки без рецепта лекарств, отпускаемых по рецепту.

Запрещенные вещества

В Google Play нельзя публиковать приложения для рекламы или продажи запрещенных веществ, даже если они заявлены как законные.

Вот примеры наиболее распространенных нарушений:

- Все продукты из неполного списка запрещенных лекарственных препаратов и пищевых добавок .
- Продукты, содержащие эфедру.
- Продукты, содержащие хорионический гонадотропин человека (ХГЧ) как средство для похудения или контроля за весом либо в сочетании с анаболическими стероидами.
- Диетические добавки и средства растительного происхождения, содержащие сильнодействующие или опасные ингредиенты.
- Продукты, в описании которых содержатся ложные заявления о пользе для здоровья, например средства, якобы сравнимые по эффективности с рецептурными лекарствами или иными подконтрольными препаратами.
- Продукты, не прошедшие государственную сертификацию, в рекламе которых подразумевается, что они безопасны или эффективны при лечении или профилактике заболеваний.
- Продукты, в отношении которых введены правительственные санкции либо приняты запретительные или предупредительные меры со стороны контролирующих органов.
- Продукты, наименования которых очень похожи на названия запрещенных пищевых добавок, фармацевтических или иных веществ с контролируемым оборотом и могут ввести в заблуждение.

Подробную информацию о запрещенных фармацевтических препаратах и пищевых добавках можно найти на сайте www.legitscript.com .

Ложная информация о здоровье

Запрещается публиковать приложения, содержащие связанные со здоровьем заявления, которые вводят в заблуждение и противоречат признанным медицинским фактам или могут причинить пользователям вред.

Вот примеры наиболее распространенных нарушений:

- Обманные утверждения о вакцинах (например, о том, что они могут изменять ДНК).
- Пропаганда опасных, неутвержденных методов лечения.
- Пропаганда других опасных медицинских процедур (например, конверсионной терапии).

1. Приложение содержит обманные утверждения, связанные со здоровьем или медициной (заявления о гарантированном предотвращении и лечении рака).

Связанные с медициной функции

Запрещено публиковать приложения со сведениями о здоровье или медицине, которые вводят в заблуждение или являются потенциально опасными. Например, запрещено размещение приложений с встроенной функцией измерения уровня кислорода. Приложения должны поддерживать связь с внешним аппаратным обеспечением, носимыми устройствами или специальными датчиками смартфонов для измерения уровня кислорода в крови. В метаданных нужно указать, что такие приложения не предназначены для медицинских целей, созданы только для общего наблюдения за здоровьем и не являются медицинскими устройствами. Кроме того, должны быть перечислены модели совместимого оборудования или устройств.

Платежи – медицинские услуги

Для транзакций, связанных с оказанием регулируемых медицинских услуг, использовать платежную систему Google Play не нужно. Подробнее о правилах Google Play в отношении платежей ...

Контент, основанный на блокчейне

По мере быстрого развития технологии блокчейн мы стремимся предоставить для разработчиков платформу, на которой они могли бы внедрять инновации и создавать более удобные и иммерсивные сервисы для пользователей.

В целях настоящего правила мы рассматриваем контент на основе блокчейна как токенизированные цифровые объекты, которые создаются и используются при помощи

технологии блокчейн. Если ваше приложение содержит такой контент, вы должны соблюдать указанные требования.

Криптовалютные биржи и программные кошельки

Чтобы покупать криптовалюты, а также владеть или обмениваться ими, необходимо использовать сертифицированные сервисы в юрисдикциях с законодательством, регулирующим обращение таких валют.

Ваше приложение также должно соответствовать действующим законам всех регионов и стран, в которых оно распространяется. Не публикуйте его в регионах или странах, где ваши продукты и сервисы запрещены. Google Play может потребовать от вас предоставить дополнительную информацию или документы о том, что ваше приложение отвечает всем действующим законам и лицензионным требованиям.

Майнинг криптовалюты

Запрещено публиковать приложения, предназначенные для майнинга криптовалют на устройствах. Приложения, регулирующие майнинг криптовалют дистанционно, разрешены.

Требования к прозрачности при распространении токенизированных цифровых объектов

Если ваше приложение продает или позволяет пользователям зарабатывать токенизированные цифровые объекты, вы должны сообщить об этом через форму декларации финансовых функций на странице "Контент приложения" в Play Console.

При создании контента для продажи через приложение вы должны указывать в сведениях о контенте, что он представляет собой токенизированный цифровой объект. Дополнительную информацию можно найти в статье Как создать контент для продажи через приложение.

Запрещается упоминать в привлекательной форме или продвигать возможность получать доход через игру или трейдинг.

Дополнительные требования к использованию NFT в игровой форме

Чтобы распространять приложения для азартных игр, работающие с токенизированными цифровыми объектами, например NFT, нужно получить разрешение, подав заявку. Это требуется согласно Правилам Google Play в отношении азартных игр, игр и соревнований с реальными денежными призами.

Во всех остальных приложениях, которые не соответствуют требованиям к приложениям для азартных игр и не указаны в разделе Другие пилотные игровые проекты с реальной валютой, никакие объекты с денежной ценностью не должны приниматься в обмен на возможность получить объекты NFT неизвестной стоимости. Объекты NFT, приобретенные пользователями, должны применяться в игре для упрощения ее прохождения и улучшения игрового процесса. Недопустимо, чтобы такие объекты использовались для ставок или заключения пари в обмен на возможность выиграть призы реальной денежной стоимости, в том числе другие объекты NFT.

Вот примеры наиболее распространенных нарушений:

- Приложения, в которых продаются наборы NFT без информации о том, какие объекты NFT в них включены и какова ценность содержимого.
- Симуляторы азартных игр, требующие оплату для начала игры и предоставляющие в качестве вознаграждения объекты NFT.

Контент, созданный искусственным интеллектом

Модели генеративного искусственного интеллекта становятся доступнее, и разработчики могут внедрять их в приложения, чтобы повышать удобство своих продуктов и вовлеченность

пользователей. Мы хотим, чтобы контент, созданный с помощью таких моделей, был безопасен для всех, а полученные отзывы учитывались при дальнейшем развитии продуктов.

Контент, созданный искусственным интеллектом

Контент, созданный искусственным интеллектом, генерируется моделями генеративного ИИ на основе запросов пользователей. Примеры:

- текст, который создается чат-ботом с генеративным ИИ в процессе общения с пользователем, если такое общение является основной функцией приложения;
- изображения и видео, которые генерируются искусственным интеллектом на основании текстовых, графических или голосовых запросов.

Для обеспечения безопасности пользователей и в соответствии со сферой действия правил Google Play приложения, создающие контент с использованием искусственного интеллекта, должны отвечать правилам для разработчиков приложений в Google Play. В частности, приложениям нельзя генерировать запрещенный контент, например способствующий эксплуатации детей или насилию над ними, а также введению в заблуждение.

Отраслевые рекомендации по обеспечению безопасности приложений на базе генеративного ИИ вы найдете в этой статье Справочного центра.

Приложения, создающие контент с помощью ИИ, должны предоставлять пользователям возможность отмечать оскорбительные материалы или сообщать о них разработчикам, не выходя из приложения. Разработчикам следует использовать жалобы пользователей в качестве источника информации для фильтрации контента и модерации в своих приложениях.

Интеллектуальная собственность

Запрещается нарушать чьи-либо права на интеллектуальную собственность (товарные знаки, авторские права, патенты, коммерческие тайны и т. д.), а также поощрять нарушение этих прав или способствовать ему. Запрет касается как приложений, так и аккаунтов разработчиков.

Если нам станет известно о подобных материалах, мы примем необходимые меры. Чтобы сообщить о нарушении авторских прав и получить дополнительную информацию, следуйте нашим инструкциям по удалению контента из Google .

Чтобы подать жалобу на приложение, в котором продаются или рекламируются поддельные товары, заполните эту форму .

Если вы владелец товарного знака и вам кажется, что он незаконно используется в приложении, которое распространяется через Google Play, рекомендуем сначала обратиться к разработчику этого приложения. Если это не поможет устранить нарушение, отправьте жалобу на незаконное использование товарного знака с помощью этой формы .

Если у вас есть письменное разрешение от правообладателя, то интеллектуальную собственность (бренд, логотип и графические объекты) можно использовать в приложении или на его странице. Обязательно свяжитесь с командой Google Play перед публикацией приложения, чтобы его не отклонили за нарушение авторских прав.

Незаконное использование контента, защищенного авторским правом

Запрещается нарушать чужие авторские права. Изменение материалов, защищенных авторским правом, также может привести к нарушению. В некоторых случаях разработчики должны доказать свое право на использование того или иного авторского контента.

Не рекомендуется использовать чужой контент для демонстрации возможностей своего приложения. Безопаснее всего создать оригинальные материалы.

Вот примеры наиболее распространенных нарушений:

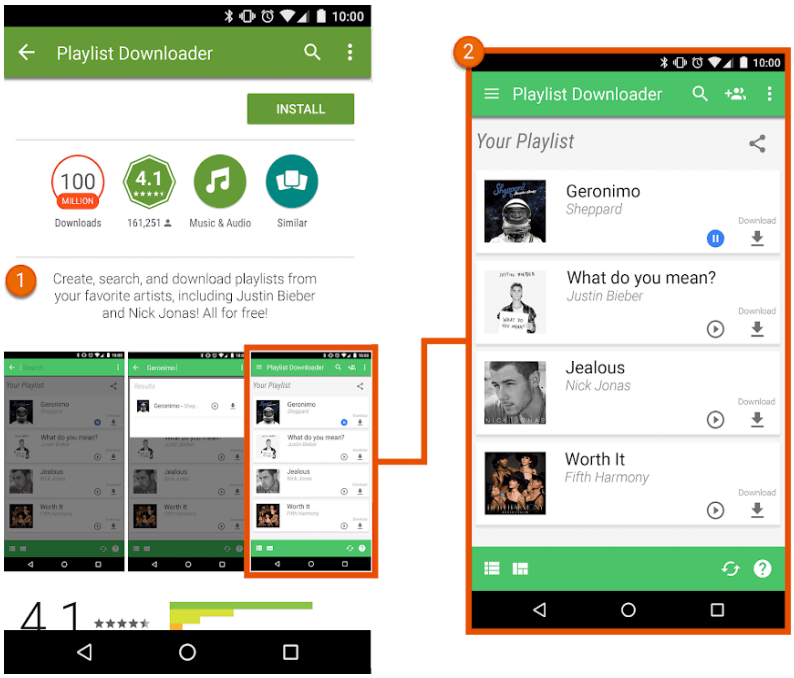
- Обложки музыкальных альбомов, видеоигр и книг.
- Рекламные изображения из фильмов, сериалов, телепередач или видеоигр.
- Изображения или заставки из комиксов, мультфильмов, фильмов, видеоклипов, сериалов или телепередач.
- Логотипы университетских или профессиональных спортивных команд.
- Фотографии из профиля известного человека в социальной сети.
- Фотографии известного человека, снятые профессиональным фотографом.
- Репродукции картин, защищенных авторским правом, или копии, неотличимые от оригинала.
- Аудиозаписи из материалов, защищенных авторским правом.
- Копии или переводы книг, не являющихся общественным достоянием.

Поощрение нарушения авторских прав

Запрещено публиковать приложения, поощряющие нарушение авторских прав или способствующие этому. Если вы не уверены, что ваше приложение не нарушает это правило, обратитесь за советом к юристу.

Вот примеры наиболее распространенных нарушений:

- Приложения для потоковой передачи видео или аудио, которые позволяют без разрешения скачать копию контента, защищенного авторским правом.
- Приложения, позволяющие слушать, смотреть и скачивать музыку, видео и другой контент в обход закона о защите авторских прав:



① В описании этого приложения пользователям предлагается скачивать контент, защищенный авторским правом, без соответствующего разрешения.
② Скриншот в описании этого приложения призывает пользователей скачивать контент, защищенный авторским правом, без соответствующего разрешения.

Нарушение прав на товарный знак

Запрещено публиковать приложения, нарушающие права на товарный знак. Товарным знаком называют слово, символ или их сочетание, указывающие на производителя товара или поставщика услуг. Он дает владельцу исключительные права на его использование применительно к данному товару или услуге.

Нарушением данных прав считается ненадлежащее или несанкционированное использование идентичного либо очень похожего товарного знака с целью дать неверное представление об источнике продукта. Если в вашем приложении присутствуют товарные знаки других продуктов, которые могут ввести пользователей в заблуждение, оно может быть заблокировано.

Поддельные товары

Запрещено публиковать приложения, в которых продаются или рекламируются поддельные товары. Речь идет об изделиях, на которых есть обозначения, идентичные чужим логотипам / товарным знакам или очень похожие на них. Это позволяет выдавать поддельный товар за подлинный.

Нарушение конфиденциальности, злоупотребление ресурсами устройства и мошенничество

Конфиденциальность пользователей и безопасность сервисов очень важны для нас. Поэтому в Google Play строго запрещается публиковать вредоносные, мошеннические и другие приложения, которые недопустимым образом используют ресурсы сети или устройства, а также персональные данные.

Данные пользователя

Вы должны точно и подробно описать, как обрабатываете пользовательские данные, например полученные от него или собранные вами, в том числе информацию с устройств. Обязательно сообщите, как и для чего вы будете собирать, обрабатывать и использовать эти данные, а также получать и предоставлять к ним доступ. Использовать такую информацию в целях, о которых вы не заявили, запрещено. Любая обработка личных и конфиденциальных пользовательских данных также должна осуществляться в рамках дополнительных требований, указанных в разделе "Личные и конфиденциальные пользовательские данные" ниже. Помимо этих и других Правил программы для разработчиков Google Play, вы должны все время соблюдать законы о защите данных и конфиденциальности, действующие в юрисдикциях, где вы распространяете свои продукты или сервисы. Например, если вы предлагаете сервисы пользователям из Европейского союза, изучите рекомендации по защите персональных данных на мобильных устройствах , принятые французским надзорным органом по защите данных (CNIL).

Если в вашем приложении есть сторонний код (например, SDK), убедитесь, что этот код, а также процессы обработки пользовательских данных на стороне его поставщика соответствуют Правилам программы для разработчиков приложений в Google Play, в том числе требованиям об использовании и раскрытии информации. Например, вы должны удостовериться, что поставщик SDK не продает личные и конфиденциальные пользовательские данные, полученные из вашего приложения. Это требование действует вне зависимости от того, передаются ли пользовательские данные после отправки на сервер или в результате внедрения стороннего кода в ваше приложение.

Личные и конфиденциальные пользовательские данные

К личным и конфиденциальным пользовательским данным относится в том числе информация, позволяющая идентифицировать личность, финансовые, платежные и учетные данные, телефонная книга, контакты, данные звонков и SMS, данные о здоровье , данные платформы "Здоровье и спорт" , данные о местоположении устройства и списке других приложений на устройстве, данные микрофона и камеры, а также другая конфиденциальная информация об устройстве или его использовании. Если ваше приложение использует такие сведения, от вас требуется следующее:

- Ограничивать доступ к личным и конфиденциальным пользовательским данным, полученным через приложение, а также их сбор, использование и передачу. Эти действия допускаются

только для предоставления функций сервиса или приложения, а также в целях, соответствующих правилам и не нарушающих обоснованные ожидания пользователей.
  - Приложения, использующие личные и конфиденциальные пользовательские данные для показа рекламы, должны соответствовать правилам размещения рекламы .
  - Данные разрешено передавать, если этого требует действующее законодательство (например, по запросу госорганов) или сделка по слиянию или продаже активов. Вы должны уведомить об этом пользователей юридически приемлемым способом. Кроме того, передача данных возможна поставщикам услуг .
- Обрабатывать все личные и конфиденциальные данные пользователей безопасным образом, в том числе с применением современных методов шифрования, например протокола HTTPS.
- По возможности запрашивать динамические разрешения, прежде чем использовать данные, доступ к которым регулируется разрешениями Android .
- Не продавать личные и конфиденциальные пользовательские данные.
  - "Продажа" подразумевает обмен или передачу таких данных третьим лицам с целью получения денежного дохода.
    - Если свои личные и конфиденциальные данные передает сам пользователь, это не считается продажей. Примеры таких ситуаций: в приложении есть функция для передачи файлов третьим лицам; приложение предназначено для проведения научных исследований, и данные отправляются в этих целях.

Раскрытие информации и разрешение на использование данных

Если ваше приложение собирает, использует и передает личные и конфиденциальные пользовательские данные в целях, которые могут не соответствовать обоснованным ожиданиям пользователей от продукта или функции (например, если сбор информации проходит в фоновом режиме), вам необходимо выполнить требования ниже.

Раскрытие информации. Вы должны указать в приложении сведения о сборе, использовании и передаче личных данных. Для таких сведений действуют следующие требования:

- Информация должна быть в самом приложении, а не только в его описании или на сайте.
- Информация должна отображаться при обычном использовании приложения, без вызова меню или настроек.
- В информации должно быть указано, какие данные использует или собирает приложение.
- В ней должно объясняться, как именно приложение использует и передает данные.
- Информация не может содержаться только в политике конфиденциальности или условиях использования.
- Информация не может включаться в состав других сведений, не связанных с вопросами сбора личных и конфиденциальных данных пользователей.

Согласие пользователей и динамические разрешения. Вы должны запросить согласие пользователя и динамическое разрешение сразу после показа сообщения о раскрытии информации, соответствующего указанным ранее правилам. Для запроса действуют следующие правила:

- Запрос должен быть сформулирован предельно ясно и представлен в отдельном диалоговом окне.
- Согласие пользователя должно подтверждаться действием (например, нажатием кнопки или установкой флажка).
- Ситуации, когда пользователь намеренно или случайно закрывает окно с запросом, в том числе нажатием в другом месте или кнопкой возврата на главный экран, не могут считаться согласием.
- Автоматически закрывающиеся запросы (например, по истечении определенного времени) не могут быть средством получения согласия.

- Запрос должен быть сначала одобрен пользователем. Только после этого ваше приложение может получить доступ к личным и конфиденциальным пользовательским данным или начать их собирать.

Приложения, в которых личные и конфиденциальные пользовательские данные обрабатываются без согласия пользователя на других правовых основаниях, должны соответствовать действующим юридическим требованиям и содержать необходимые сообщения о раскрытии информации, в том числе сообщения в самих приложениях, требуемые согласно этим правилам. Таким основанием может быть законный интерес в рамках Генерального регламента ЕС о защите персональных данных (GDPR).

Чтобы привести приложение в соответствие правилам, мы рекомендуем вам придерживаться следующего формата, когда требуется раскрыть информацию:

- "[Название приложения] собирает/передает/синхронизирует/хранит [тип данных], чтобы обеспечить работу [какой функции] [в каких случаях]".
- *Пример. "Fitness Funds собирает данные о местоположении, чтобы отслеживать вашу физическую активность, даже когда приложение закрыто или не используется, и чтобы поддерживать показ рекламы".*
- *Пример. "Call Buddy собирает, считывает и записывает данные о вызовах, чтобы иметь доступ к контактам, даже когда приложение не используется".*

Если в вашем приложении используется сторонний код (например, SDK), предназначенный для сбора личных и конфиденциальных пользовательских данных, вы должны предоставить достаточные доказательства того, что ваше приложение не нарушает требования из раздела "Раскрытие информации и разрешение на использование данных" настоящих правил. Приложение должно соответствовать в том числе положениям, связанным с доступом к данным, а также их сбором, использованием и передачей с помощью стороннего кода. Доказательства необходимо отправить в течение двух недель или другого периода (если он указан) после получения запроса от Google Play.

Вот примеры наиболее распространенных нарушений:

- Приложение собирает данные о местоположении устройства, но не содержит заметного уведомления об использовании их приложением в фоновом режиме и/или о том, для какой функции нужны эти данные.
- Приложение запрашивает динамическое разрешение на доступ к данным до раскрытия информации о том, для чего используются эти данные.
- Приложение получает доступ к списку установленных приложений пользователя и не обрабатывает эти данные как личные или конфиденциальные в соответствии с политикой конфиденциальности, правилами обработки данных, а также согласно требованиям к раскрытию информации и разрешению на использование данных.
- Приложение получает доступ к списку контактов пользователя и не обрабатывает эти данные как личные или конфиденциальные в соответствии с политикой конфиденциальности, а также требованиями к обработке данных и разрешению на использование данных.
- Приложение записывает данные, которые появляются на экране, и не обрабатывает их как личные или конфиденциальные в соответствии с настоящими правилами.
- Приложение собирает данные о местоположении устройства , не раскрывая, для чего они нужны, и не получая согласие пользователя в соответствии с приведенными выше требованиями.
- Приложение использует ограниченные разрешения в фоновом режиме (в том числе для отслеживания или в исследовательских или маркетинговых целях), не раскрывая, для чего они требуются, и не получая согласие пользователя в соответствии с приведенными выше требованиями.
- Приложение использует SDK, который собирает личные и конфиденциальные пользовательские данные и не обрабатывает их согласно правилам в отношении

пользовательских данных, требованиям к раскрытию информации и разрешению на использование данных, а также требованиям к обработке данных (включая запрет на продажу).

Подробнее о раскрытии информации и разрешении на использование данных...

Ограничение доступа к личным и конфиденциальным данным

Ниже перечислены дополнительные требования к приложениям, выполняющим определенные функции.

Функция	Требования
Обработка идентификационных, финансовых и платежных данных	Ваше приложение не должно ни при каких обстоятельствах публиковать личные и конфиденциальные данные, связанные с финансовой или платежной деятельностью, а также номера официальных удостоверений личности.
Обработка телефонных номеров и другой контактной информации	Запрещено без разрешения публиковать и раскрывать личную и конфиденциальную информацию других людей.
Антивирусные и другие защитные функции	В политике конфиденциальности и информации об использовании личных данных должно объясняться, какие данные собираются и передаются, как они используются и кто может получить к ним доступ.
Детский контент	В приложении, предназначенном в том числе и для детей, не должны использоваться SDK, которые не одобрены для подобных сервисов. С полным списком правил и требований можно ознакомиться на этой странице .
Сбор постоянных идентификаторов устройств (например, IMEI, IMSI, серийных номеров SIM-карт и т. д.)	Постоянные идентификаторы устройства не должны быть связаны с личными и конфиденциальными данными пользователя и с идентификаторами, которые могут быть сброшены, за исключением: • телефонной связи с помощью SIM-карты (например, для звонков по сети Wi-Fi через оператора связи); • корпоративных приложений для управления устройствами, используемых в режиме владельца. В таких случаях разработчик должен явным образом сообщить пользователям об использовании идентификаторов в соответствии с правилами в отношении пользовательских данных . Информацию об альтернативных уникальных идентификаторах можно найти на этой странице . Дополнительные рекомендации по использованию рекламных идентификаторов Android приведены в правилах размещения рекламы .

Раздел безопасности данных

Каждое приложение должно содержать раздел безопасности данных, в котором понятно и точно описано, как собираются, используются и передаются пользовательские данные. Разработчик несет ответственность за точность и актуальность информации. Эти сведения должны соответствовать информации, изложенной в политике конфиденциальности приложения (если применимо).

Подробнее о том, как заполнить раздел безопасности данных ...

Политика конфиденциальности

Ссылка на политику конфиденциальности должна быть приведена в предназначенном для нее разделе Play Console и в самом приложении (допускается разместить текст правил). В этом документе и в информации об использовании данных, размещенной в приложении, должно

подробно объясняться, как оно получает, собирает, использует и передает третьим лицам пользовательские данные. Это касается любой информации, а не только сведений, описанных в разделе безопасности данных. Текст должен содержать:

- информацию о разработчике, а также о контактном лице по вопросам конфиденциальности или о механизме подачи запросов;
- типы личных и конфиденциальных пользовательских данных, которые доступны приложению и которые оно собирает, использует и передает, а также сведения о том, кто получает доступ к этой информации;
- информацию о процедурах безопасной обработки личных и конфиденциальных данных;
- правила разработчика в отношении хранения и удаления данных;
- четкое указание на то, что это политика конфиденциальности (например, может быть упомянуто в заголовке).

В политике конфиденциальности необходимо привести название приложения или упомянуть лицо (например, разработчика или компанию), указанное на странице приложения в Google Play. Даже если приложение не имеет доступа к личным и конфиденциальным данным, у него должна быть политика конфиденциальности.

Убедитесь, что этот документ (не в виде PDF-файла) доступен по активной общедоступной ссылке без ограничений по геозоне и не может быть изменен.

Требование в отношении удаления аккаунтов

Если пользователи могут создавать аккаунты прямо в вашем приложении, в нем также должна быть возможность запрашивать удаление аккаунта. Такую опцию должно быть легко найти в приложении. Кроме того, пользователи должны иметь возможность запросить удаление аккаунта не из приложения, например на вашем сайте. Ссылку на такой ресурс нужно указать в соответствующем поле формы URL в Play Console.

При удалении аккаунта в приложении по запросу пользователя вы также должны удалить пользовательские данные, связанные с этим аккаунтом. Временная деактивация, отключение или приостановка работы аккаунта не считаются удалением. Если вам нужно хранить определенную информацию в обоснованных целях, например для обеспечения безопасности, борьбы с мошенничеством или соблюдения нормативных требований, вы обязаны явно проинформировать пользователей о своих правилах хранения данных, например в политике конфиденциальности.

Подробнее о требованиях в отношении удаления аккаунтов и об изменении формы "Безопасность данных"...

Использование идентификатора приложения

Android представит новый идентификатор для основных примеров использования, например аналитики и предотвращения мошенничества. Условия использования идентификатора приведены ниже.

- **Использование.** Идентификатор набора приложений нельзя использовать для персонализации и анализа рекламы.
- **Связь с информацией, позволяющей идентифицировать личность, и другими идентификаторами.** Идентификатор набора приложений нельзя связывать в рекламных целях с идентификаторами Android (например, AAID) или с какими-либо персональными и конфиденциальными данными.
- **Прозрачность и согласие.** В примечании о конфиденциальности, соответствующем требованиям законодательства, в том числе в политике конфиденциальности, необходимо проинформировать пользователя о сборе и использовании идентификаторов приложения, а также о настоящих правилах. В некоторых случаях необходимо получить согласие пользователей. Подробная информация о наших стандартах конфиденциальности приведена в разделе Данные пользователя .

Рамочные соглашения о конфиденциальности данных между ЕС, США, Великобританией и Швейцарией

Если вы получаете доступ к личным данным пользователей, предоставленным компанией Google и созданным на территории Европейской экономической зоны, Великобритании или Швейцарии (далее – Персональные данные, созданные в ЕС), если используете или обрабатываете эту информацию и по ней можно прямо или косвенно установить личность человека, то вы должны:

- Соблюдать все действующие законы, директивы, регламенты и правила в отношении конфиденциальности, безопасности и защиты данных.
- Получать доступ к личным данным и использовать их только в тех целях, с которыми согласился их владелец.
- Применять необходимые организационные и технические средства для защиты Персональных данных, созданных в ЕС, от потери, недопустимого использования, несанкционированного или незаконного доступа, раскрытия, изменения и уничтожения.
- Обеспечивать необходимый уровень защиты информации в соответствии с принципами рамочного соглашения о конфиденциальности данных или использовать действующий механизм передачи данных согласно Условиям Google в отношении защиты данных при взаимодействии между контролерами данных.

Вы обязаны регулярно сверяться с этими требованиями. Если соблюдать их станет невозможно или возникнет серьезный риск того, что вы не сможете обеспечить соответствие им, немедленно сообщите нам об этом по адресу data-protection-office@google.com и сразу прекратите обработку Персональных данных, созданных в ЕС, или как можно скорее восстановите необходимый уровень их защиты.

Разрешения и API с доступом к конфиденциальной информации

Запросы на предоставление разрешений и использование API, которые получают доступ к конфиденциальной информации, должны быть понятными для пользователей. Запрашивать разрешения и использовать API, которые получают доступ к конфиденциальной информации, можно только в том случае, если они необходимы для работы функций и сервисов, которые уже есть в приложении и описаны на его странице в Google Play. Нельзя использовать разрешения и API, предоставляющие доступ к данным пользователя или устройства, для функций или целей, которые не отмечены в описании приложения, не реализованы или не разрешены. Личные или конфиденциальные данные, полученные с разрешения пользователя или при помощи таких API, нельзя продавать и передавать с целью последующей продажи ни при каких обстоятельствах.

Запрашивайте разрешения в контексте (по мере возникновения необходимости в них), чтобы пользователи понимали, зачем это нужно приложению. Используйте данные только в тех целях, на которые пользователь дал согласие. Если в дальнейшем вам понадобится использовать их в других целях, вам необходимо будет получить явное согласие пользователя на это.

Ограниченные разрешения

Кроме того, к разрешениям, которые указаны ниже или обозначены в документации для разработчиков как опасные , специальные или требующие особой подписи , применяются дополнительные требования и ограничения:

- Данные пользователя и устройства, полученные с помощью ограниченных разрешений, считаются личной и конфиденциальной информацией, на которую распространяются правила в отношении пользовательских данных .
- Если пользователь отклоняет запрос на ограниченное разрешение, вы не должны пытаться переубедить его. Нельзя заставлять пользователей предоставлять разрешения, которые не являются критически важными. В этом случае вы обязаны приложить обоснованные усилия для того, чтобы все равно обеспечить пользователям доступ к функциям приложения (например,

предусмотреть возможность ввода телефонного номера вручную, если доступ к списку вызовов ограничен).

- Строго запрещено использовать разрешения в целях, не соответствующих правилам Google Play в отношении вредоносного ПО (включая злоупотребление повышенными привилегиями).

Для некоторых ограниченных разрешений могут действовать дополнительные требования, описанные ниже. Соблюдение этих условий помогает обеспечивать конфиденциальность пользователей. В очень редких случаях мы можем сделать исключение, если приложение выполняет какие-либо важные и востребованные функции, которые в настоящий момент не могут быть реализованы другим способом. Принимая решение в таких ситуациях, мы учитываем потенциальные угрозы конфиденциальности и безопасности данных.

Разрешения на доступ к SMS и списку вызовов

SMS и список вызовов считаются личными и конфиденциальными данными. К ним применяются положения раздела Личная и конфиденциальная информация , а также следующие ограничения:

Ограниченное разрешение	Требования
Группа разрешений на доступ к списку вызовов (например, READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Приложение должно быть зарегистрировано как помощник или обработчик звонков по умолчанию.
Группа разрешений на доступ к SMS (например, READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	Приложение должно быть зарегистрировано как помощник или обработчик SMS по умолчанию.

Приложениям, которые не могут быть назначены помощником или обработчиком SMS или звонков по умолчанию, запрещено запрашивать подобные разрешения. В том числе нельзя указывать соответствующие теги в манифесте. Запрашивать такие разрешения можно только после того, как пользователь сам установит приложение в качестве помощника или обработчика для SMS или звонков по умолчанию. Как только пользователь изменит свой выбор, приложение должно прекратить использовать эти разрешения. Допустимые сценарии использования и исключения описаны в этой статье Справочного центра .

Приложения могут использовать указанные выше разрешения и полученные благодаря им данные только для работы основных функций (например, для обеспечения возможностей, явно указанных в описании приложения). Основными называются функции, без которых приложение невозможно использовать. Передача данных, в том числе для использования по лицензии, а также предоставление доступа к ним допускается только в целях, необходимых для работы основных функций приложения или сервисов в нем. Запрещено использовать данные в любых других целях, включая улучшение сервисов или приложений, рекламу и маркетинг. Нельзя использовать альтернативные способы (включая другие разрешения, API и сторонние источники) для получения данных, связанных с разрешениями на доступ к списку вызовов и SMS.

Разрешения на доступ к данным о местоположении

Данные о местоположении устройства считаются личными и конфиденциальными. К ним применяются положения правил о личной и конфиденциальной информации и доступе к данным о местоположении в фоновом режиме, а также следующие требования:

- Приложения не должны использовать данные, защищенные разрешениями на доступ к местоположению (например, `ACCESS_FINE_LOCATION`, `ACCESS_COARSE_LOCATION`, `ACCESS_BACKGROUND_LOCATION`), если эти сведения не нужны для работы функций и сервисов, которые уже есть в приложении.

- Ни при каких обстоятельствах нельзя запрашивать доступ к данным о местоположении, если они будут использоваться только для рекламы и аналитики. Приложения, в которых эти данные будут использоваться в том числе для показа рекламы (после получения разрешения от пользователя), должны соответствовать правилам размещения рекламы .
- Запрашивать следует минимально необходимый уровень доступа (то есть доступ к приблизительным, а не к точным данным о местоположении и разрешение на использование в активном режиме, а не в фоновом) и только если доступ действительно требуется для работы сервиса или функции, имеющихся в приложении. Пользователи должны ясно понимать, почему для той или иной функции нужен запрашиваемый уровень доступа. Мы можем отказать в публикации приложений, которые запрашивают фоновый доступ к данным о местоположении без веского обоснования.
- Доступ к данным о местоположении в фоновом режиме можно использовать только в том случае, если они нужны для работы функций, которые полезны для пользователя и связаны с основным назначением приложения.

Приложение может получать доступ к сведениям о местоположении в активном режиме (когда с приложением работают), если использование этих данных:

- необходимо для выполнения в приложении действия, инициированного пользователем;
- прекращается сразу после выполнения этого действия.

Приложения, разработанные специально для детей, должны соответствовать требованиям программы Приложения для всей семьи .

Дополнительную информацию можно найти в этой справочной статье .

Разрешение на доступ ко всем файлам

Информация о файлах и папках на устройстве пользователя считается личной и конфиденциальной информацией и должна соответствовать положениям раздела Личная и конфиденциальная информация , а также следующим требованиям:

- Приложения должны запрашивать доступ к хранилищу устройства только в том случае, если это необходимо для работы приложения. Они не могут запрашивать доступ к хранилищу от имени третьего лица для любых целей, не связанных с ключевыми функциями приложения.
- Устройствам Android с версией R или более поздней для управления доступом к общему хранилищу необходимо разрешение `MANAGE_EXTERNAL_STORAGE` . Все приложения, предназначенные для этой версии системы и запрашивающие доступ к общему хранилищу ("Доступ ко всем файлам"), проходят соответствующую проверку перед публикацией. Приложения, которые могут использовать это разрешение, должны явно предлагать пользователям включить доступ ко всем файлам в меню настроек "Специальный доступ для приложений". Дополнительную информацию можно найти в этой статье .

Разрешение на доступ к списку пакетов (приложений)

Список установленных приложений на устройстве пользователя считается личной и конфиденциальной информацией, на которую распространяются положения раздела Личная и конфиденциальная информация , а также следующие требования:

Приложения, основной функцией которых является запуск, поиск других приложений на устройстве или взаимодействие с ними, могут получить соответствующее разрешение на просмотр других установленных приложений следующим образом:

- **Широкий доступ к списку пакетов.** Это возможность приложения видеть все установленные на устройстве приложения (пакеты).
  - Приложения с целевым уровнем API 30 или выше могут получить широкий доступ к списку установленных приложений с помощью разрешения `QUERY_ALL_PACKAGES` , только когда

для корректной работы приложения необходимо получать данные о других приложениях на устройстве и/или взаимодействовать с ними.

- Нельзя использовать разрешение QUERY_ALL_PACKAGES, если приложение может работать с более ограниченным набором пакетов . Например, вы можете выбрать отдельные пакеты, доступ к которым будет запрашивать ваше приложение.

- Использование альтернативных методов для обеспечения широкого доступа, близкого к тому, который можно получить с помощью разрешения QUERY_ALL_PACKAGES, допускается только для работы основных пользовательских функций приложения, а также для взаимодействия с приложениями, найденными этими методами.
- О том, в каких случаях можно использовать разрешение QUERY_ALL_PACKAGES, рассказано в этой статье Справочного центра .

- **Ограниченный доступ.** Приложение с ограниченным доступом будет запрашивать только информацию об определенных приложениях, применяя более строгие методы, например с помощью указанных параметров в файле манифеста. Этот метод можно использовать, когда приложение соответствует правилам и ему нужно управлять другими приложениями или взаимодействовать с ними.
- Доступ к списку установленных приложений должен быть напрямую связан с основным назначением или основными пользовательскими функциями приложения.

Ни при каких обстоятельствах нельзя продавать данные о списке приложений, полученные от приложений из Google Play, а также предоставлять доступ к этой информации для аналитики и получения дохода от рекламы.

API для специальных возможностей

API для специальных возможностей нельзя использовать:

- для изменения настроек пользователя без его согласия или блокировки отключения или удаления приложений или сервисов, за исключением случаев, когда разрешение было предоставлено родителем или законным представителем через приложение родительского контроля или уполномоченными администраторами через программное обеспечение для управления корпоративными устройствами;
- для работы в обход настроек конфиденциальности, встроенных в операционную систему Android;
- для модификации пользовательского интерфейса или взаимодействия с ним в нарушение правил Google Play для разработчиков (например, с целью обмана пользователей).

API для специальных возможностей не предназначен для удаленной записи звонков и не может запрашиваться для этой цели.

Использование API для специальных возможностей должно быть отмечено на странице приложения в Google Play.

Рекомендации по использованию метода IsAccessibilityTool

Если основным назначением приложения является непосредственная поддержка людей с инвалидностью, вы можете указать, что это ПО для обеспечения специальных возможностей, выполнив метод **IsAccessibilityTool**.

В противном случае вы не можете использовать этот метод, но приложение все равно должно соответствовать требованиям к раскрытию информации и получению согласия пользователей, описанным в правилах в отношении пользовательских данных , поскольку поддержка специальных возможностей неочевидна. Чтобы узнать больше, прочитайте статью об AccessibilityService API в нашем Справочном центре.

Используйте API и разрешения с более узкой областью действия, чем у API для специальных возможностей, если этого достаточно для желаемой функциональности.

Разрешение "Запрос пакетов установки"

Разрешение `REQUEST_INSTALL_PACKAGES` позволяет запрашивать установку пакетов приложений. Для его использования требуются следующие основные функции:

- отправка и получение пакетов приложений;
- установка пакетов приложений по команде пользователя.

Допускается наличие следующих функций:

- просмотр веб-страниц или веб-поиск;
- обмен сообщениями с возможностью прикрепления файлов;
- передача и совместное использование файлов, а также управление ими;
- управление корпоративными устройствами;
- резервное копирование и восстановление;
- перенос данных с одного устройства на другое;
- синхронизация телефона с носимым устройством или устройством IoT (например, с умными часами или Smart TV) через сопутствующее приложение.

Основная функция – это главное назначение приложения. Она должна быть явно обозначена в описании приложения.

Разрешение `REQUEST_INSTALL_PACKAGES` нельзя использовать для обновления, изменения или объединения других APK в файле объекта. Это можно сделать только в целях управления устройством. Обновление и установка пакетов должны выполняться по инициативе и под контролем пользователя в соответствии с правилами Google Play в отношении злоупотребления ресурсами устройства и сети.

Разрешения использовать данные нательных датчиков

Данные датчиков, измеряющих физические параметры тела (например, пульс, SpO_2 и температуру кожи), считаются конфиденциальной пользовательской информацией**.** На приложения, которые запрашивают доступ к этим сведениям, распространяются правила в отношении пользовательских данных и приложений для здоровья. Эти правила действуют для разрешений `android.permission.BODY_SENSORS` и `android.permission.BODY_SENSORS_BACKGROUND` на устройствах всех типов, в том числе телефонах, планшетах и устройствах Wear OS.

Начиная с ОС Android 16 вместо единого разрешения `BODY_SENSORS` будут использоваться отдельные разрешения для конкретных типов данных `android.permissions.health.*` (например, `android.permission.health.READ_HEART_RATE`, `android.permission.health.READ_OXYGEN_SATURATION`, `android.permission.health.READ_SKIN_TEMPERATURE`). Это позволит повысить конфиденциальность информации.

В приложениях для Android 16 или более поздней версии при доступе к API, для которых ранее требовалось `BODY_SENSORS`, нужно будет использовать отдельные разрешения. Подробнее...

Персональные конфиденциальные данные можно собирать только в одобренных целях и в интересах пользователя. Поэтому мы будем проверять все запросы на устаревшие и новые разрешения, касающиеся нательных датчиков. К допустимым вариантам использования в первую очередь относится отслеживание физической формы (например, запись тренировок в реальном времени), заболеваний и самочувствия, а также исследования в области здравоохранения (при наличии необходимых одобрений) и оптимизация функций сопутствующих приложений для носимых устройств.

Подробнее о правилах, требованиях, а также разрешенных и запрещенных примерах использования...

Разрешения Android для Health Connect

Здоровье и спорт – это одна из платформ Android, которая позволяет приложениям для отслеживания здоровья и физической активности хранить данные на устройстве и обмениваться ими в рамках единой экосистемы. В этом сервисе пользователи также могут разрешать и запрещать приложениям записывать и считывать информацию о здоровье и двигательной активности. Информация о здоровье может включать в себя анамнез, диагнозы, назначенные лекарства и иные виды лечения, результаты лабораторных исследований и другие клинические данные, полученные от медицинских организаций или через поддерживаемые сторонние платформы.

Платформа "Здоровье и спорт" поддерживает запись и чтение данных различных типов , например сведений о температуре тела, количестве шагов и информации о здоровье.

Данные, доступ к которым осуществляется через разрешения для платформы "Здоровье и спорт", считаются персональной и конфиденциальной пользовательской информацией. К ним применяются правила в отношении пользовательских данных. Если ваш продукт относится к приложениям для здоровья или у него есть связанные со здоровьем функции и доступ к информации о здоровье, в том числе к данным платформы "Здоровье и спорт", он также должен соответствовать правилам в отношении приложений для здоровья.

Если вы хотите использовать платформу "Здоровье и спорт" в своем приложении, прочитайте руководство для разработчиков Android . Узнайте, как запросить доступ к нужным типам данных с этой платформы, и получите ответы на другие часто задаваемые вопросы о разрешениях.

Чтобы приложения, распространяемые в Google Play, могли считывать и записывать информацию на платформе "Здоровье и спорт", они должны соответствовать указанным ниже требованиям.

Разрешенные цели доступа к платформе Health Connect и ее использования

Использовать платформу "Здоровье и спорт" можно только при соблюдении действующих правил и условий использования и в целях, указанных в этих правилах. То есть запрашивать разрешения можно, если ваше приложение или сервис относится к одной из одобренных категорий.

Одобрены следующие категории: физическая активность и здоровый образ жизни, награды, рекомендации фитнес-тренеров, корпоративное здоровье, медицинская помощь, исследования в области здравоохранения и игры. Приложениям из этих категорий, получившим разрешения, нельзя использовать их для незаявленных или запрещенных целей.

Запрашивать разрешения на доступ к данным платформы "Здоровье и спорт" могут только приложения или сервисы, в которых есть хотя бы одна функция, предназначенная для того, чтобы помогать пользователям следить за здоровьем и физической активностью. К ним относятся:

- Приложения и сервисы, позволяющие пользователям **напрямую отмечать в журнале, включать в отчеты, отслеживать и/или анализировать** физические характеристики, медицинские показатели, информацию о своей физической активности, сне, психическом здоровье, питании и/или другие сведения и показатели, связанные со здоровьем или двигательной активностью.
- Приложения и сервисы, позволяющие пользователям **сохранять физические характеристики, медицинские показатели, информацию о своей физической активности, сне, психическом здоровье, питании** и/или другие сведения и показатели, связанные со здоровьем или двигательной активностью, на своем устройстве и делиться этой информацией с другими приложениями на устройстве, которые используют данные в разрешенных целях.
- Приложения и сервисы, позволяющие пользователям отслеживать течение хронических заболеваний, прием лекарственных средств или получение сопутствующей поддержки.

Запрещается получать доступ к данным платформы "Здоровье и спорт" с нарушением этих правил или других действующих условий использования или правил в отношении платформы "Здоровье и спорт", в том числе:

- Не используйте ее для разработки приложений, сред или операций или интеграции в них таких данных, если использование платформы "Здоровье и спорт" или сбой в ее работе может с достаточной вероятностью приводить к порче имущества, смерти, травме и ущербу для физических лиц или окружающей среды (например, для создания или эксплуатации атомных электростанций, в системах управления полетами, системах жизнеобеспечения или вооружениях).
- Не используйте ее данные в приложениях без графического интерфейса. У каждого приложения должен быть хорошо заметный значок, который отображается на панели приложений, в настройках приложений на устройстве, в уведомлениях и т. д.
- Не используйте ее в приложениях, которые синхронизируют данные между несовместимыми устройствами или платформами.
- Не используйте ее для подключения к приложениям, сервисам или функциям, предназначенным исключительно для детей.
- Принимайте разумные и необходимые меры для защиты приложений и систем, взаимодействующих с данными платформы "Здоровье и спорт", от несанкционированного и незаконного доступа, использования, уничтожения, потери, изменения или раскрытия.

Вы также должны соблюдать все нормативные и юридические требования, которые могут применяться к вам с учетом предполагаемого использования платформы "Здоровье и спорт" и любых данных, полученных из этого сервиса. Например, если на вас или на партнера вашего бизнеса распространяется действие закона США "О преемственности страхования и отчетности в области здравоохранения" (HIPAA), вы обязаны соблюдать применимые требования в отношении доступа к информации с платформы "Здоровье и спорт" и использования этих сведений. Если на вас, как на разработчика, распространяется действие Генерального регламента о защите персональных данных (GDPR) в отношении пользователей из ЕС, вы должны выполнять предусмотренные им обязательства. Действующее законодательство может предусматривать, что с лицами, участвующими в обработке информации, до ее передачи должны быть заключены дополнительные соглашения, например соглашение между деловыми партнерами или об обработке данных. Также разработчики обязаны самостоятельно устанавливать, необходимы ли эти документы для их операций, и по запросу предоставлять Google подтверждение того, что соглашения заключены или требования соблюдены.

Если в предоставленной Google маркировке или сопроводительной информации для определенных продуктов и сервисов Google явно не указано иное, Google не гарантирует точность данных платформы "Здоровье и спорт" и не подтверждает их пригодность для любых целей и, в частности, для исследований, здравоохранения и медицины. Google отказывается от любой ответственности, связанной с использованием данных платформы "Здоровье и спорт".

Ограничение использования

В отношении доступа к данным платформы "Здоровье и спорт" и их использования действуют описанные ниже ограничения.

- Данные могут использоваться только в целях предоставления или улучшения разрешенных возможностей и функций, которые видны в интерфейсе приложения.
- Передавать третьим лицам данные пользователя можно исключительно с его явного согласия и только в следующих целях: обеспечение безопасности (например, разбирательство в отношении недопустимого использования сервисов), соблюдение действующего законодательства или предоставление информации в результате слияния или поглощения.
- Люди могут получать доступ к данным пользователя только с его явного согласия, если это требуется для обеспечения безопасности, соблюдения законов или (в агрегированной форме и в соответствии с юридическими требованиями) для внутренних операций.

- **Запрещается передача, использование или продажа данных платформы "Здоровье и спорт" в любых других целях, включая перечисленные ниже.**
  - Передача или продажа пользовательских данных третьим лицам, таким как рекламные платформы, брокеры данных и другие продавцы информации.
  - Передача, продажа или использование пользовательских данных для показа рекламы, включая персонализированные объявления и рекламу на основе интересов.
  - Передача, продажа или использование пользовательских данных для определения платежеспособности или предоставления кредита.
  - Передача, продажа или использование пользовательских данных с любым продуктом или сервисом, который может квалифицироваться как медицинское изделие. Исключениями являются случаи, когда приложение медицинского изделия соответствует всем действующим законам, в том числе если регулирующие органы, такие как Управление США по санитарному надзору за качеством пищевых продуктов и медикаментов (FDA), предоставили необходимые разрешения и одобрили использование данных платформы "Здоровье и спорт" в заявленных целях, а пользователи предоставили явное согласие на это.
  - Передача, продажа или использование пользовательских данных в каких-либо целях или каким-либо способом, затрагивающим закрытую информацию о состоянии здоровья (см. определение такой информации в законе США "О преемственности страхования и отчетности в области здравоохранения" (HIPAA)), кроме случаев, когда такие операции инициированы пользователем и соответствуют требованиям HIPAA.

Минимальная сфера применения

Запрашивать можно только те разрешения, которые требуются для работы функций или сервисов в вашем продукте. Запросы доступа должны быть конкретными и касаться лишь необходимых данных.

Понятное и точное заявление и описание

На платформе "Здоровье и спорт" хранится информация о физической активности и здоровье, включая персональные и конфиденциальные данные. Разработчики обязаны понятно рассказать, как они работают с данными, в подробной политике конфиденциальности и обеспечить доступ к этой информации. В отношении раскрываемых сведений должны соблюдаться следующие требования:

- Точно указаны приложение или сервис, запрашивающие доступ к пользовательским данным.
- Приведено понятное и исчерпывающее описание типов данных, которые запрашиваются, собираются или к которым осуществляется доступ. Данные связаны с пользовательской функцией или рекомендацией, предлагаемой в приложении.
- Разъяснено, как данные будут использоваться и/или передаваться. Если вы запрашиваете их с одной целью, а они используются для чего-то ещё, необходимо уведомить пользователей обо всех целях.
- Предоставлена справочная информация о том, как пользователи могут управлять своими данными (в том числе удалять их) в приложении и что происходит с данными после деактивации или удаления аккаунта.
- Указано, как обеспечивается безопасность при обработке личных и конфиденциальных данных пользователей, в том числе рассказано о передаче этой информации с применением современных методов шифрования, например протокола HTTPS.

Подробнее о требованиях к приложениям, подключающимся к платформе "Здоровье и спорт"...

VPN-сервис

VpnService – это базовый класс, который позволяет создавать собственные решения VPN в приложениях или расширять их функциональность. Создавать безопасный туннель от устройства к удаленному серверу могут только приложения, которые используют VpnService и основная функция которых связана с организацией VPN-подключения. Это ограничение не распространяется на приложения, для работы основных функций которых требуется удаленный сервер, например:

- приложения для родительского и корпоративного контроля;
- средства мониторинга использования приложений;
- решения для защиты устройств (например, антивирусное ПО, средства управления мобильными устройствами, брандмауэр);
- сетевые инструменты (например, для удаленного доступа);
- приложения для просмотра веб-страниц;
- приложения операторов, которым для предоставления телефонной связи требуется VPN.

Запрещается использовать класс VpnService в следующих целях:

- сбор персональных и конфиденциальных данных пользователей без раскрытия информации об этом и получения согласия;
- перенаправление пользовательского трафика из других приложений на устройстве или манипулирование им с целью монетизации (например, направление рекламного трафика через страну, отличную от страны, где находится пользователь);

Приложения, в которых используется VpnService, должны:

- содержать соответствующее упоминание на странице приложения в Google Play;
- шифровать данные, которые передаются с устройства на конечную точку туннеля VPN;
- соответствовать Правилам программы для разработчиков, в том числе правилам в отношении мошенничества с рекламой, разрешений и вредоносного ПО.

Разрешение на выполнение операций в точное время

Мы представляем новое разрешение `USE_EXACT_ALARM`, которое позволяет работать с функцией выполнения операций в точное время в приложениях с целевой версией ОС не ниже Android 13 (API уровня 33).

`USE_EXACT_ALARM` – это ограниченное разрешение. Оно должно объявляться в приложениях, только если для работы их основных функций требуется выполнение операций в точное время. Если в ходе обязательной проверки выясняется, что приложения, запрашивающие ограниченное разрешение, не соответствуют критериям допустимого использования, они снимаются с публикации на Google Play.

Допустимое использование разрешения на выполнение операций в точное время

Разрешение `USE_EXACT_ALARM` можно указывать, только если для работы основных функций приложения, важных для пользователя, требуется выполнять действия в точное время. Например, если:

- приложение выполняет функции будильника или таймера;
- приложение выполняет функции календаря с уведомлениями о событиях.

Если вашему приложению требуется функция выполнения операций в точное время, не указанная выше, возможно, вам подойдет разрешение `SCHEDULE_EXACT_ALARM`.

Подробнее о выполнении операций в точное время...

Разрешение на отправку полноэкранных уведомлений намерений

Чтобы использовать разрешение `USE_FULL_SCREEN_INTENT` в приложениях, поддерживающих Android 14 (целевой уровень API 34) и более новые версии ОС, требуется специальный доступ. Это разрешение автоматически предоставляется приложениям, для основных функций которых нужны уведомления высокого приоритета. Такими функциями могут быть:

- установка будильника;
- прием видеовызовов и телефонных звонков.

Приложения, запрашивающие это разрешение, подлежат проверке. Если они не соответствуют критериям выше, разрешение `USE_FULL_SCREEN_INTENT` не будет предоставляться им автоматически. В таком случае приложения должны запрашивать его у пользователя.

Обратите внимание, что использование разрешения `USE_FULL_SCREEN_INTENT` должно соответствовать всем правилам Google Play для разработчиков, в том числе требованиям в отношении рекламы, нежелательного ПО для мобильных устройств и злоупотребления ресурсами устройства и сети. Полноэкранные уведомления, запускаемые с помощью намерений, не должны вредить устройству пользователя, получать к нему несанкционированный доступ, нарушать работу этого устройства и вмешиваться в нее. Также недопустимо, чтобы приложения с этим разрешением вмешивались в работу других приложений и негативно влияли на удобство использования устройства.

Узнать больше о разрешении `USE_FULL_SCREEN_INTENT` можно в Справочном центре.

Age Signals API и пользовательские данные

В этих правилах описаны условия использования Age Signals API, который предоставляет доступ к личным и конфиденциальным данным о возрасте пользователей и родительском согласии.

Данные, полученные через Age Signals API, можно использовать только для того, чтобы соблюдать действующие юридические или нормативные обязательства, например обеспечивать в приложении возможности, соответствующие возрасту пользователей.

Вам строго запрещено использовать эти данные в определенных целях, включая, помимо прочего:

- рекламу, маркетинг и персонализацию, в том числе показ объявлений с таргетингом;
- анализ данных, профилирование пользователей и бизнес-аналитику;
- продажу, передачу или раскрытие данных третьим лицам по любой причине, кроме случаев, когда это строго требуется по закону.

Злоупотребление ресурсами устройства и сети

Запрещается публиковать приложения, которые нарушают работу устройства пользователя, других устройств, компьютеров, серверов, сетей, API или сервисов (включая другие приложения на устройстве, сервисы Google и сети операторов связи), а также вмешиваются в их работу, получают несанкционированный доступ к ним или вредят иным образом.

Приложения, размещаемые в Google Play, должны соответствовать требованиям оптимизации для Android, зафиксированным в Основных критериях качества приложений.

Приложения, которые распространяются в Google Play, не должны изменять свой код каким-либо способом, кроме обновления через Google Play. Они также не должны скачивать исполняемый

код (например, файлы в формате DEX, JAR или SO) из каких-либо источников, кроме Google Play. Это правило не распространяется на код, который запускается на виртуальной машине или интерпретаторе и имеет ограниченный доступ к API Android (например, код JavaScript в компоненте WebView или браузере).

Приложения или сторонний код (например, SDK), использующие интерпретируемые языки (JavaScript, Python, Lua и т. д.), которые загружаются во время работы (а не загружены в приложение изначально), не должны нарушать правила Google Play.

Запрещено использовать код, который создает или использует уязвимости безопасности. Информация о самых актуальных проблемах безопасности содержится в нашей Программе повышения безопасности приложений для разработчиков.

Вот примеры наиболее распространенных нарушений:

Примеры распространенных злоупотреблений ресурсами устройства и сети:

- Приложения, которые прерывают показ рекламы в других приложениях.
- Приложения, которые влияют на геймплей в играх, например позволяют жульничать.
- Приложения, которые помогают взламывать сервисы, ПО или устройства и обходить защитные системы или содержат инструкции о том, как это делать.
- Приложения, которые нарушают условия использования сервисов или API.
- Приложения, которые пытаются обойти ограничения по управлению питанием (кроме разрешенных случаев).
- Приложения, которые предоставляют услуги прокси-сервера третьим лицам (разрешено, только когда это является основной функцией приложения).
- Приложения или сторонний код (например, SDK), которые скачивают исполняемый код, например DEX-файлы или нативный код из источника, отличного от Google Play.
- Приложения, которые устанавливают на устройство другие приложения, не получив заранее согласие пользователя.
- Приложения, которые содержат ссылки на вредоносное ПО или способствуют его распространению или установке.
- Приложения или сторонний код (например, SDK), которые содержат компонент WebView с интерфейсом JavaScript и загружают ненадежный веб-контент (например, URL с протоколом HTTP) или непроверенные URL, полученные из ненадежных источников, например из ненадежных намерений.
- Приложения, которые используют разрешение для полноэкранных объектов intent, чтобы вынуждать пользователя взаимодействовать с объявлениями или уведомлениями, прерывающими работу приложения.
- Приложения, которые обходят защиту изолированных сред Android, чтобы собирать данные о действиях или личности пользователя из других приложений.

Использование активных служб

Разрешение на запуск активных служб обеспечивает надлежащее использование таких служб. Если приложение предназначено для Android 14 или более поздней версии, вы должны указать допустимые типы для всех используемых в нем активных служб. Для каждого типа также потребуется объявить подходящее разрешение на запуск активной службы. Например, если в приложении используется определение местоположения на карте, в манифесте нужно указать разрешение FOREGROUND_SERVICE_LOCATION.

Объявлять в приложении разрешение на запуск активных служб можно только в следующих случаях:

- Служба требуется функции, которая полезна для пользователя и связана с основным назначением приложения.

- Служба запускается пользователем, или ее работа заметна для него. Например, служба воспроизводит песню, транслирует медиаконтент на другое устройство, предоставляет точные и понятные уведомления или по запросу пользователя загружает фото в облако.
- Пользователь может завершить или остановить работу службы.
- Если выполнение службы будет прервано или отложено, это вызовет у пользователя негативную реакцию или функция будет работать не так, как предполагалось (например, когда нужно позвонить, система не должна откладывать вызов).
- Служба работает не дольше, чем требуется для выполнения задачи.

Критерии выше не распространяются на следующие типы активных служб:

- systemExempted и shortService ;
- dataSync (только при использовании функций Play Asset Delivery).

Подробнее об использовании активных служб...

Передача данных, инициированная пользователем

API для передачи данных, инициированной пользователем, может запускаться в приложениях, только если:

- задача инициируется пользователем;
- данные передаются по сети;
- задача выполняется не дольше, чем требуется для передачи данных.

Подробнее об API для передачи данных, инициированной пользователем...

Требования к использованию параметра FLAG_SECURE

Указанный в коде приложения флаг FLAG_SECURE позволяет ограничить демонстрацию конфиденциальных данных в продукте, например исключить создание скриншотов с ними или просмотр таких сведений на незащищенных экранах. Объявляйте этот флаг, если контент приложения не следует транслировать, показывать или передавать другим образом за пределы приложения или устройства пользователя.

По соображениям безопасности и конфиденциальности все приложения, которые распространяются через Google Play, должны учитывать наличие FLAG_SECURE в других приложениях. Это значит, что запрещается создавать способы обхода параметра FLAG_SECURE в других приложениях или способствовать их использованию.

Это требование не затрагивает приложения, которые считаются инструментами специальных возможностей , если они не передают, не сохраняют и не кешируют контент, защищенный флагом FLAG_SECURE, для предоставления доступа к таким данным вне устройства пользователя.

Приложения с локальными контейнерами Android

Приложения с локальными контейнерами Android позволяют создавать среду, которая частично или полностью имитирует ОС Android. Такая среда может содержать не все функции безопасности Android , поэтому разработчики могут добавить в файл манифеста параметр, сообщающий локальным контейнерам Android, что приложение не должно запускаться в имитируемой ими среде.

Параметр в манифесте, обеспечивающий безопасность среды

Параметр REQUIRE_SECURE_ENV в манифесте позволяет указать, что это приложение нельзя запускать в локальном контейнере Android. По соображениям безопасности и

конфиденциальности приложения, предоставляющие локальные контейнеры Android, должны учитывать наличие этого параметра в других приложениях, а также:

- Проверять манифесты приложений, загружаемых в локальный контейнер Android, на наличие этого параметра.
- Не загружать в локальный контейнер Android приложения, в манифестах которых объявлен этот параметр.
- Не выступать в качестве прокси-сервера, перехватывая или вызывая API на устройстве, чтобы они казались установленными в контейнере.
- Не создавать и не помогать использовать методы обхода этого параметра (например, загружая более раннюю версию приложения, чтобы обойти действующий параметр REQUIRE_SECURE_ENV).

Узнать больше об этих правилах можно в нашем Справочном центре.

Введение в заблуждение

Мы запрещаем публиковать приложения, которые пытаются ввести пользователей в заблуждение или способствуют недобросовестной деятельности, включая приложения, заявленные функции которых невозможно реализовать на устройстве. Информация о приложении, его описание, а также фото и видео должны соответствовать его функциональности. Приложения не должны имитировать функции или предупреждения операционной системы и других программ. Любые изменения настроек устройства должны производиться с ведома и согласия пользователя. Кроме того, у пользователя должна быть возможность отменить изменения.

Заявления, вводящие в заблуждение

Скриншоты, значки, названия, описания и другие материалы приложения не должны содержать ложную или вводящую в заблуждение информацию.

Вот примеры наиболее распространенных нарушений:

- Описание функций приложения вводит в заблуждение или не соответствует действительности:
  - Согласно описанию и скриншотам игра является гонкой, однако в действительности представляет собой головоломку из блоков, в которой используется картинка машины.
  - Согласно описанию приложение является антивирусом, хотя в действительности содержит только рекомендации о том, как удалять вирусы.
- В описании приложения указаны невыполнимые функции (например, отпугивание насекомых), даже если оно представлено как шутка или розыгрыш.
- Приложение отнесено к неправильной категории (например, может быть неверно указано возрастное ограничение).
- Приложение содержит явно недостоверный контент, связанный с результатами голосования или способный повлиять на его процесс.
- В описании приложения содержатся ложные заявления о том, что оно связано с государственными учреждениями, предоставляет государственные услуги или оказывает содействие в их получении, при этом приложение не было надлежащим образом одобрено для этих целей.
- Приложение ложно представлено как официальный продукт известной компании. Запрещается использовать такие названия, как "От Димы Билана", "Официально от Димы Билана" и подобные, без соответствующих прав.

2. Для приложения заявлены невыполнимые функции (например, использование телефона в качестве алкотестера).

Несанкционированные изменения настроек устройства

Запрещается публиковать приложения, которые вносят изменения в настройки устройства или другие приложения без ведома и согласия пользователя. К настройкам устройства относятся параметры системы и браузера, закладки, ярлыки, значки и виджеты приложений на главном экране.

Кроме того, запрещено указанное ниже.

- Приложения, которые изменяют настройки или функции устройства с согласия пользователя, но таким образом, что это нельзя легко отменить.
- Приложения и содержащиеся в них объявления, которые каким-либо образом добавляют на устройство рекламу или ссылки на сервисы третьих сторон.
- Приложения, которые обманным путем побуждают пользователя удалять или деактивировать программы других разработчиков либо изменять настройки устройства.
- Приложения, которые призывают пользователей удалять или отключать программы других разработчиков либо изменять настройки устройства. Исключение составляют приложения, обеспечивающие безопасность устройства или данных.

Пособничество недобросовестной деятельности

Запрещается публиковать приложения, которые рассчитаны на использование в недобросовестных целях. Например, приложения для создания паспортов и других удостоверений личности, номеров социального страхования, дипломов, кредитных карт,

банковских счетов и водительских прав. Информация о приложении, его название, описание, а также изображения и видеоролики должны соответствовать его реальным функциям и содержанию, а само приложение должно работать так, как этого ожидает пользователь.

Дополнительные ресурсы приложения (например, игровые объекты) могут быть доступны для скачивания, только если они необходимы для использования приложения. При этом они должны соответствовать всем правилам Google Play, а приложение должно сообщать пользователю размер этих файлов до начала скачивания.

Заявления о том, что приложение создано для розыгрышей и в других развлекательных целях, не избавляют разработчиков от ответственности и необходимости соблюдать наши правила.

Вот примеры наиболее распространенных нарушений:

- Приложения, которые копируют интерфейс других приложений или веб-сайтов, чтобы обманом получить персональные или учетные данные.
- Приложения, в которых указаны непроверенные или реальные адреса, номера телефонов и идентификационные данные людей или компаний, размещенные без согласия этих лиц или организаций.
- Приложения, основные функции которых меняются в зависимости от места проживания пользователя, параметров устройства или других данных пользователя, если эти различия не указаны в явном виде в описании приложения.
- Приложения, которые сильно изменяются в зависимости от версии без уведомления пользователя (например, в разделе Что нового) и обновления описания.
- Приложения, которые изменяют или скрывают свои функции во время проверки.
- Приложения, которые выполняют скачивание через сеть доставки контента (CDN), предварительно не сообщая пользователю размер скачиваемых файлов.

Манипулирование медиаконтентом

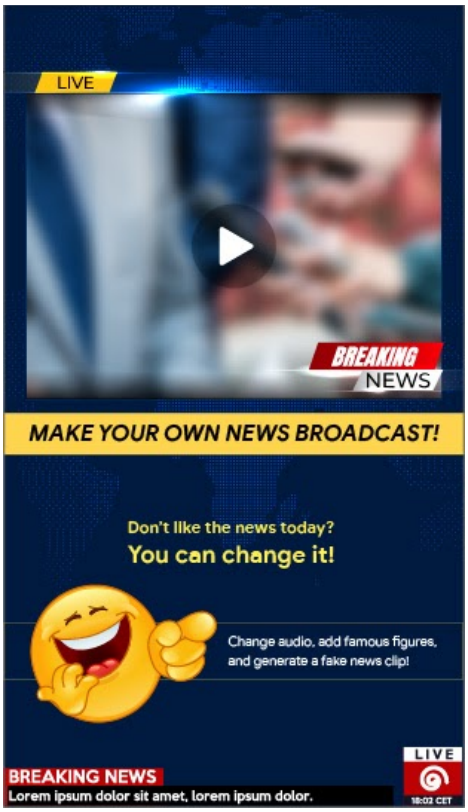
Запрещено публиковать приложения, которые способствуют распространению ложной или вводящей в заблуждение информации в виде изображений, аудио, видео или текста. Не разрешены приложения, распространяющие заведомо ложные или вводящие в заблуждение изображения, текст или видео, которые могут нанести вред в связи с событиями, требующими деликатного отношения, политикой, социальными вопросами и другими общественно значимыми темами.

Исключения могут быть сделаны для информации, представляющей общественный интерес, отредактированного медиаконтента с заявлениями для пользователей или водяными знаками, очевидных примеров сатиры или пародии, а также для изображений, явно созданных искусственным образом.

Отредактированные медиаматериалы должны соответствовать правилам для разработчиков приложений в Google Play, в том числе положениям о запрещенном контенте.

Вот примеры наиболее распространенных нарушений:

- Приложения, на страницах которых в Google Play используются изображения событий, требующих деликатного отношения, или известных людей, с целью продемонстрировать функции изменения медиаконтента.
- Приложения для редактирования видео, позволяющие имитировать выпуски новостей, добавив названия и логотипы реальных новостных агентств без явного отказа от обязательств или водяного знака.
- Приложения, единственное предназначение которых – создание вводящего в заблуждение медиаконтента.



1. С помощью этого приложения можно редактировать видео, имитируя выпуски новостей, а также добавлять в клипы изображения знаменитостей и общественных деятелей без водяного знака.

Прозрачность поведения

Пользователям должно быть понятно, что делает ваше приложение. Не используйте в нем скрытые, неактивные или незадокументированные функции. Запрещено пытаться избежать проверки приложений какими-либо способами. Чтобы обеспечить безопасность пользователей, целостность системы и соответствие правилам, может потребоваться дополнительная информация о приложении.

Искажение фактов

Мы запрещаем приложения и аккаунты разработчиков, которые:

- выдают себя за других лиц или другие организации, а также скрывают или искажают свою основную цель или сведения о владельцах;
- намеренно вводят пользователей в заблуждение, например скрывают или искажают информацию о стране происхождения или предоставляют контент пользователям в других странах;
- сотрудничают с другими приложениями, сайтами, разработчиками и аккаунтами в целях сокрытия или фальсификации данных о приложении или разработчике, а также другой важной информации (это относится к контенту, который имеет политическую, социальную или общественную направленность).

Правила Google Play в отношении целевого уровня API

Чтобы обеспечить безопасность пользователей, для **всех приложений** в Google Play необходимо установить следующие целевые уровни API:

Обновления и новые приложения должны использовать уровень Android API не ниже выпущенного в течение года перед выходом последней основной версии Android. Публикация в Play Console приложений и обновлений, которые не удовлетворяют этому требованию, будет отклонена.

Размещенные в Google Play приложения, для которых не выпускаются обновления и в которых установлен уровень API ниже опубликованного в течение двух лет перед выходом последней основной версии Android, будут недоступны новым пользователям на устройствах с более поздними версиями ОС Android. Те, кто ранее устанавливал такие приложения из Google Play, смогут находить, переустанавливать и использовать их на устройствах с любой версией ОС Android, поддерживаемой приложением.

Технические рекомендации о том, как перейти на новый целевой уровень API в соответствии с требованиями, можно найти в нашем руководстве .

О точных сроках и случаях-исключениях рассказано в этой справочной статье .

Правила в отношении пользовательских данных

К данным пользователя относятся сведения, предоставленные им, а также полученные в ходе его работы, в том числе информация об устройстве. Обязательно сообщите, как и для чего вы будете собирать, обрабатывать и использовать эти данные, а также получать и предоставлять к ним доступ. Использовать такую информацию в целях, о которых вы не заявили, запрещено.

Если в вашем приложении используется сторонний код (например, SDK), убедитесь, что он сам и реализованные в нем процессы обработки пользовательских данных соответствуют Правилам программы для разработчиков приложений в Google Play, в том числе требованиям об использовании и раскрытии информации. Например, вы должны удостовериться, что поставщик SDK не продает личные и конфиденциальные данные пользователя, полученные из вашего приложения. Это требование применяется вне зависимости от того, как будут переданы пользовательские данные: после отправки на сервер или в результате внедрения стороннего кода в ваше приложение.

Личные и конфиденциальные пользовательские данные

- Ограничивайте доступ к личным и конфиденциальным пользовательским данным, полученным через приложение, а также их сбор, использование и передачу. Эти действия допускаются только для предоставления функций сервиса или приложения, а также в целях, соответствующих правилам и не нарушающих обоснованные ожидания пользователей.
  - Приложения, использующие личные и конфиденциальные пользовательские данные для показа рекламы, должны соответствовать правилам Google Play в отношении размещения рекламы.
- Все личные и конфиденциальные данные пользователей должны обрабатываться безопасным образом, в том числе с применением современных методов шифрования, например протокола HTTPS.
- Прежде чем использовать данные, доступ к которым регулируется разрешениями Android, приложение должно запросить динамическое разрешение (всегда, когда это возможно).

Продажа личных и конфиденциальных пользовательских данных

Не продавайте личные и конфиденциальные пользовательские данные.

- Продажа подразумевает передачу информации третьим лицам или обмен ею с целью получения денежного дохода.
  - Если свои личные и конфиденциальные данные передает сам пользователь, это не считается продажей. Примеры таких ситуаций: в приложении есть функция для передачи файлов третьим лицам; приложение предназначено для проведения научных исследований, и данные отправляются в этих целях.

Раскрытие информации и разрешение на использование данных

Если ваше приложение собирает, использует, передает личные и конфиденциальные пользовательские данные или получает доступ к ним в целях, которые могут не соответствовать обоснованным ожиданиям

пользователей от продукта или функции, необходимо соблюдать требования к раскрытию информации и получению разрешения на использование данных, указанные в правилах в отношении таких данных.

Если в вашем приложении применяется сторонний код (например, SDK), предназначенный для сбора личных и конфиденциальных пользовательских данных, вы должны предоставить достаточные доказательства того, что приложение не нарушает требования из раздела "Раскрытие информации и разрешение на использование данных" настоящих правил. Приложение должно соответствовать, в частности, положениям о доступе к данным, их сборе, использовании и передаче с помощью стороннего кода. Доказательства необходимо отправить в течение двух недель или другого периода (если он указан) после получения запроса от Google Play.

Обязательно удостоверьтесь, что в стороннем коде (например, SDK) не нарушаются правила в отношении пользовательских данных.

С более подробной информацией о требованиях к раскрытию информации и получению согласия пользователей можно ознакомиться в Справочном центре.

Примеры нарушений, вызванных SDK

- Приложение использует SDK, который собирает личные и конфиденциальные пользовательские данные и не обрабатывает их согласно правилам в отношении пользовательских данных, требованиям к раскрытию информации и разрешению на использование данных, а также требованиям, касающимся доступа к данным и их обработки (включая запрет на продажу).
- В приложение интегрирован SDK, который собирает личные и конфиденциальные пользовательские данные по умолчанию, что нарушает требования настоящих правил в отношении раскрытия информации и получения согласия пользователей.
- Для приложения заявлено, что оно собирает личные и конфиденциальные пользовательские данные только для обеспечения работы функций, защищающих от мошенничества и злоупотреблений, но SDK также передает собранные данные третьим лицам в рекламных целях или для аналитики.
- Приложение содержит SDK, который передает сведения об установленных пакетах с нарушением рекомендаций по раскрытию информации и/или требований политики конфиденциальности.
  - Чтобы узнать больше, прочитайте правила в отношении нежелательного ПО для мобильных устройств.

Дополнительные требования в отношении доступа к личным и конфиденциальным данным

В таблице ниже представлены требования к определенным функциональным особенностям приложений.

Функциональная особенность	Требования
Сбор постоянных идентификаторов устройств (IMSI, IMEI-кодов, серийных номеров SIM-карт и т. д.) или установка связи с такими идентификаторами	Постоянные идентификаторы устройств не должны быть связаны с личными и конфиденциальными данными пользователей или сбрасываемыми идентификаторами устройств, за исключением следующих ситуаций: • когда это требуется для услуг телефонии с привязкой к идентификационным данным SIM-карты (например, для звонков по сети Wi-Fi через оператора связи); • в корпоративных приложениях, предназначенных для управления устройствами и используемых в режиме владельца. В этих случаях разработчик должен явным образом сообщить пользователям о связи с идентификаторами согласно правилам в отношении пользовательских данных. Информацию об альтернативных уникальных идентификаторах можно найти на этой странице . Дополнительные рекомендации по использованию рекламных идентификаторов Android приведены в правилах размещения рекламы.

Приложение предназначено для детей	В приложения разрешено включать только SDK, которые прошли самостоятельную сертификацию для использования в сервисах, предназначенных для детей. Ознакомьтесь с полной версией правил и требований Программы самостоятельной сертификации рекламных SDK в приложениях для всей семьи.

Примеры нарушений, вызванных SDK

- Приложение использует SDK, который связывает IMEI-код и данные о местоположении.
- Приложение работает с SDK, который связывает рекламный идентификатор Android с постоянными идентификаторами устройства в рекламных целях или для аналитики.
  В приложение интегрирован SDK, который связывает рекламный идентификатор Android с адресом электронной почты в целях аналитики.

Раздел безопасности данных

Каждое приложение должно содержать раздел безопасности данных, в котором понятно и точно описано, как собираются, используются и передаются пользовательские данные. Это также относится к данным, которые собираются и обрабатываются через сторонние библиотеки или SDK, используемые в приложениях. Разработчик несет ответственность за точность и актуальность такой информации. Сведения в этом разделе должны соответствовать тому, что указано в политике конфиденциальности приложения (если применимо).

Изучите дополнительную информацию о том, как заполнить раздел безопасности данных, в Справочном центре.

Ознакомьтесь также с полной версией правил в отношении пользовательских данных.

Правила использования разрешений и API с доступом к конфиденциальной информации

Запросы на предоставление разрешений и использование API, которые получают доступ к конфиденциальной информации, должны быть понятными для пользователей. Запрашивать разрешения и использовать API, которые получают доступ к конфиденциальной информации, можно только в том случае, если они необходимы для работы уже внедренных функций и сервисов, описанных на странице приложения в Google Play. Нельзя использовать разрешения и API, предоставляющие доступ к данным пользователя или устройства, для функций или целей, которые не отмечены в описании приложения, не реализованы или не разрешены. Личные или конфиденциальные данные, полученные с разрешения пользователя или при помощи таких API, нельзя продавать и передавать с целью последующей продажи ни при каких обстоятельствах.

Ознакомьтесь с полной версией правил использования разрешений и API с доступом к конфиденциальной информации.

Примеры нарушений, вызванных применением SDK

- В приложение интегрирован SDK, который запрашивает доступ к данным о местоположении в фоновом режиме для запрещенных или незаявленных целей.
- Приложение использует SDK, который без согласия пользователя передает IMEI-код, полученный с помощью разрешения read_phone_state в Android.

Правила в отношении вредоносного ПО

Основной принцип простой: экосистема Android, включающая Google Play и устройства пользователей, не должна подвергаться воздействию вредоносного ПО. Руководствуясь им, мы стараемся делать экосистему Android безопасной для пользователей и их устройств Android.

Вредоносным ПО считается любой код, который может представлять угрозу для пользователя, а также его данных или устройств. Например, к вредоносному ПО относятся потенциально опасные приложения (ПОП), а также исполняемые файлы и модификации фреймворков,

относящиеся к таким категориям, как троянские программы, фишинговое и шпионское ПО. Мы постоянно обновляем этот список и добавляем новые категории.

Эти правила также применяются к стороннему коду (например, SDK), который включен в приложение.

Ознакомьтесь с полной версией правил в отношении вредоносного ПО.

Примеры нарушений, вызванных применением SDK

- Приложение содержит библиотеки SDK от поставщиков, распространяющих вредоносное ПО.
- Приложение нарушает модель разрешений Android или крадет учетные данные (такие, как токены OAuth) из других приложений.
- Приложения злоупотребляют функциями, чтобы препятствовать удалению или остановке.
- Приложение отключает SELinux.
- Приложение использует SDK, который нарушает модель разрешений Android, получая повышенные привилегии для незаявленной цели благодаря доступу к данным устройства.
- Приложение содержит SDK с кодом, который обманным путем заставляет пользователей приобретать подписки или оплачивать контент через оператора мобильной связи.

Использование SDK в приложениях

Если вы хотите добавить сторонний SDK, то должны убедиться в том, что его код и реализованные в нем процессы не нарушают Правила программы для разработчиков приложений в Google Play. Важно знать, как SDK в приложении обрабатывают пользовательские данные. Кроме того, следует понимать, какие разрешения они используют, какие сведения собирают и почему.

Требования к SDK

Разработчики приложений часто используют сторонний код (например, SDK), чтобы интегрировать важные функции и сервисы в свои продукты. Включая SDK в приложение, важно убедиться, что безопасность пользователей не пострадает и в коде не появятся новые уязвимости. В этом разделе мы объясним, как некоторые из наших актуальных требований к конфиденциальности и безопасности применяются в отношении SDK и каким образом они должны помогать разработчикам безопасно интегрировать SDK в приложения.

Если вы хотите добавить сторонний SDK, то должны убедиться в том, что его код и реализованные в нем процессы не нарушают Правила программы для разработчиков приложений в Google Play. Важно знать, как SDK в приложении обрабатывают пользовательские данные. Кроме того, следует понимать, какие разрешения они используют, какие сведения собирают и почему. Помните о том, что сбор и обработка пользовательских данных со стороны SDK должны соответствовать политике приложения.

Чтобы не допустить нарушений, изучите весь текст следующих правил и обратите внимание на актуальные требования в отношении SDK, которые приведены ниже.

Приложения, которые без разрешения пользователя получают root-доступ через повышение привилегий, относятся к категории "Получение root-доступа".

Шпионское ПО

Шпионским ПО называют вредоносное приложение, код или поведение, которые позволяют собирать, получать или передавать третьим лицам данные пользователя или устройства, когда это не связано с функциями, соответствующими правилам.

К шпионскому ПО также относится вредоносный код или поведение, которые могут считаться способами слежки за пользователем или получают данные не уведомляя его и не получая его согласия.

Вы можете ознакомиться с полной версией правил в отношении шпионского ПО.

Нарушение правил в отношении шпионского ПО будет считаться вызванным SDK, в частности, в следующих случаях:

- если в приложении используется SDK, который передает данные из аудиозаписей или записей звонков, когда это не связано с функциями, соответствующими правилам;
- если в приложении используется вредоносный сторонний код (например, SDK), который передает данные с устройства неожиданным для пользователя способом и/или не уведомляя его и не получая его согласия.

Правила в отношении нежелательного ПО для мобильных устройств

Понятная функциональность и явное раскрытие информации

Любой код должен исполнять всё, что обещано пользователю. Приложения должны выполнять все заявленные функции и не должны вводить пользователей в заблуждение.

Примеры нарушений:

- мошенничество с рекламой;
- социальная инженерия.

Защита пользовательских данных

Понятно и подробно расскажите о том, как приложение получает доступ к личным и конфиденциальным данным пользователя, как оно их собирает, использует и передает. При работе с такой информацией необходимо соблюдать все применимые правила в отношении пользовательских данных, а также принимать меры предосторожности для защиты этих сведений.

Примеры нарушений:

- сбор данных (шпионское ПО);
- нарушение ограниченных разрешений.

Ознакомьтесь с полной версией правил в отношении нежелательного ПО для мобильных устройств.

Правила в отношении злоупотребления ресурсами устройства и сети

Запрещаются приложения, которые нарушают работу устройства пользователя, других устройств, компьютеров, серверов, сетей, API или сервисов (включая другие приложения на устройстве, сервисы Google и сети операторов связи), а также вмешиваются в их работу, получают несанкционированный доступ к ним или вредят иным образом.

Приложения или сторонний код (например, SDK), использующие интерпретируемые языки (JavaScript, Python, Lua и т. д.), которые загружаются во время работы (а не загружены в приложение изначально), не должны нарушать правила Google Play.

Запрещено использовать код, который создает или использует уязвимости безопасности. Информация о самых актуальных проблемах безопасности содержится в нашей Программе повышения безопасности приложений для разработчиков.

Ознакомьтесь с полной версией правил в отношении злоупотребления ресурсами устройства и сети.

Примеры нарушений, вызванных применением SDK

- Приложение предоставляет услуги прокси-сервера третьим лицам (кроме случаев, когда это является основной функцией приложения).
- В приложение интегрирован SDK, который скачивает исполняемый код (например, DEX-файлы или нативный код) не из Google Play.
- В приложение интегрирован SDK, который содержит компонент WebView с интерфейсом JavaScript, загружающий ненадежный веб-контент (например, URL с протоколом HTTP) или непроверенные URL, полученные из ненадежных источников (например, URL из ненадежных объектов Intent).
- В приложение интегрирован SDK, который содержит код, используемый для обновления собственного APK.
- В приложение интегрирован SDK, который скачивает файлы через незащищенное соединение, чем подвергает риску безопасность пользователя.
- В приложении используется SDK с кодом, который позволяет скачивать или устанавливать приложения из неизвестных источников вне Google Play.
- В приложение интегрирован SDK, который использует активные службы без обоснованной причины.
- В приложение интегрирован SDK, который использует активные службы в целях, соответствующих правилам, но не объявлен в файле манифеста.

Правила в отношении введения в заблуждение

Мы запрещаем публиковать приложения, которые пытаются ввести пользователей в заблуждение или способствуют недобросовестной деятельности, включая приложения, заявленные функции которых невозможно реализовать на устройстве. Информация о приложении, его описание, а также фото и видео должны соответствовать его функциональности. Приложения не должны имитировать функции или предупреждения операционной системы и других программ. Любые изменения настроек устройства должны производиться с ведома и согласия пользователя. Кроме того, у пользователя должна быть возможность отменить изменения.

Ознакомьтесь с полной версией правил в отношении введения в заблуждение.

Прозрачность поведения

Пользователям должно быть понятно, что делает ваше приложение. Не используйте в нем скрытые, неактивные или незадокументированные функции. Запрещено пытаться избежать проверки приложений какими-либо способами. Чтобы обеспечить безопасность пользователей, целостность системы и соответствие правилам, может потребоваться дополнительная информация о приложении.

Пример нарушения, связанного с применением SDK

- В приложение интегрирован SDK, позволяющий избежать проверки приложений.

Какие правила Google Play для разработчиков обычно связаны с нарушениями, вызванными применением SDK?

Удостоверьтесь в том, что весь сторонний код, который использует ваше приложение, соответствует Правилам программы для разработчиков в Google Play. Для этого изучите следующие материалы:

- Правила в отношении пользовательских данных
- Разрешения и API с доступом к конфиденциальной информации
- Правила в отношении злоупотребления ресурсами устройства и сети
- Вредоносное ПО
- Нежелательное ПО для мобильных устройств
- Программа самостоятельной сертификации рекламных SDK в приложениях для всей семьи

- Правила размещения рекламы
- Введение в заблуждение
- Правила программы для разработчиков приложений в Google Play

Выше перечислены правила, которые не соблюдаются чаще всего. Однако из-за ненадежного кода SDK ваше приложение может нарушить и другое правило, не вошедшее в этот список. Изучайте правила полностью и следите за их обновлениями. Ведь именно разработчик приложения несет ответственность за то, чтобы SDK обрабатывали данные приложения в соответствии с правилами.

Подробную информацию можно найти в нашем Справочном центре.

Вредоносное ПО

Основной принцип простой: экосистема Android, включающая Google Play и устройства пользователей, не должна подвергаться воздействию вредоносного ПО. Руководствуясь им, мы стараемся делать экосистему Android безопасной для пользователей и их устройств Android.

Вредоносным ПО считается любой код, который может представлять угрозу для пользователя, а также его данных или устройств. Например, к вредоносному ПО относятся потенциально опасные приложения (ПОП), а также исполняемые файлы и модификации фреймворков, относящиеся к таким категориям, как троянские программы, фишинговое и шпионское ПО. Мы постоянно обновляем этот список и добавляем новые категории.

Эти правила также применяются к стороннему коду (например, SDK), который включен в приложение.

Вредоносные программы могут различаться по типу и принципу действия, но, как правило, преследуют какие-либо из следующих целей:

- вмешательство в работу устройства пользователя;
- получение контроля над устройством пользователя;
- выполнение удаленных операций, позволяющих получать доступ к зараженному устройству или каким-либо образом использовать его;
- передача персональных или учетных данных с устройства без ведома и согласия пользователя;
- рассылка с зараженного устройства спама или команд, которые затрагивают другие устройства или сети;
- мошеннические действия по отношению к пользователю.

Приложения, исполняемые файлы и модификации фреймворков, даже если они изначально не были созданы с вредоносными целями, могут считаться потенциально опасными и представлять угрозу для пользователя. Дело в том, что они могут действовать по-разному в зависимости от целого ряда факторов. Компоненты, которые могут представлять риск для одних устройств Android, совершенно безвредны для других. Например, вредоносные программы, использующие устаревшие API, не станут угрозой для устройств, на которых установлена последняя версия ОС Android, в отличие от устройств с более ранними версиями. Приложения, исполняемые файлы и модификации фреймворков помечаются как вредоносные или потенциально опасные, если они представляют явную угрозу для некоторых или всех пользователей и устройств Android.

Мы хотим, чтобы наша экосистема была безопасной, построенной на инновациях и доверии, а также чтобы пользователи понимали, как именно злоумышленники могут эксплуатировать их устройства. Именно поэтому мы подготовили описание категорий вредоносного ПО.

Подробную информацию можно найти на сайте Google Play Защиты .

Бэкдоры

Код, который позволяет удаленно выполнять на устройстве нежелательные, потенциально опасные операции.

Такие операции могут включать процессы, из-за автоматического выполнения которых приложение, исполняемый файл или модификация фреймворка попадет в другие категории вредоносного ПО. В целом бэкдор – это способ, с помощью которого потенциально опасные операции могут быть выполнены на устройстве. Поэтому бэкдор сложно поставить в один ряд с такими категориями, как мошенническое списание средств или коммерческое шпионское ПО. В результате Google Play Защита при определенных обстоятельствах может посчитать набор бэкдоров уязвимостью.

Мошенническое списание средств

Код, который приводит к автоматическому списанию средств пользователя обманным способом.

Существует три категории мошеннических списаний средств через операторов мобильной связи: SMS- и телефонное мошенничество, а также мошенничество с оформлением подписки или оплатой контента.

SMS-мошенничество
В этом случае код приводит к отправке платных SMS без согласия пользователя или скрывает соглашения, содержащие информацию о передаче SMS, или сообщения, в которых оператор связи уведомляет о списании средств или подтверждает оформление подписки.

Бывает, что код не скрывает от пользователя отправку сообщений, но способствует SMS-мошенничеству другими путями. Примеры: сокрытие определенных разделов соглашения с информацией о передаче SMS или представление этих разделов в нечитаемом виде, блокировка сообщений, в которых оператор связи уведомляет пользователя о списании средств или подтверждает подписку.

Мошенничество со звонками
В этом случае код приводит к звонкам на платные номера без согласия пользователя.

Мошенничество с оформлением подписки или оплатой контента
В этом случае код используется для того, чтобы обманным путем заставить человека приобрести подписку или оплатить контент через оператора мобильной связи.

К этой категории относятся все списания средств, кроме тех, которые вызваны платными SMS и звонками. Примеры: оплата через оператора или по протоколу WAP и передача минут мобильной связи. Мошенничество с WAP особенно распространено. Оно может использоваться для того, чтобы обманом заставить человека нажать кнопку в незаметно загружающемся прозрачном компоненте WebView. В результате подписка оформляется, а SMS или письмо с подтверждением транзакции перехватывается, чтобы пользователь не узнал о списании средств.

ПО для преследования

Программный код, который в целях мониторинга собирает персональные или конфиденциальные пользовательские данные с устройства и передает их третьим лицам (компаниям или физическим лицам).

Приложения должны раскрывать информацию и получать согласие в соответствии с правилами в отношении пользовательских данных .

Рекомендации в отношении приложений для мониторинга

Единственными приемлемыми приложениями для мониторинга являются приложения, предназначенные для родительского или корпоративного контроля. При этом должны полностью соблюдаться приведенные ниже требования. С помощью этих приложений запрещается следить за другими лицами (например, за супругом или супругой) даже с ведома и согласия таких лиц и при условии показа уведомления о передаче информации. Чтобы объявить, что приложение

используется для мониторинга, в файле манифеста необходимо указать параметр IsMonitoringTool.

Приложения для мониторинга должны соответствовать перечисленным ниже требованиям.

- В описании приложения не должно говориться, что это шпионское ПО или инструмент для секретной слежки.
- Приложения не должны скрывать свои функции отслеживания или вводить пользователя в заблуждение по этому поводу.
- Во время работы таких приложений должны постоянно отображаться уведомление о том, что приложение запущено, и уникальный значок, позволяющий однозначно идентифицировать приложение.
- В описании приложения в Google Play должны упоминаться его функции мониторинга или отслеживания.
- В приложениях и на их страницах в Google Play не должно быть способов активировать функции, нарушающие эти правила, или получить доступ к таким функциям. Например, запрещены ссылки на не соответствующие требованиям APK-файлы, размещенные не в Google Play.
- Приложения должны соответствовать действующему законодательству. Вы несете полную ответственность за соблюдение законов страны, где ваше приложение будет распространяться.

Подробную информацию вы найдете в справочной статье об использовании флага isMonitoringTool .

Атака типа "отказ в обслуживании" (DoS)

Код, который незаметно для пользователя запускает атаку типа "отказ в обслуживании" (DoS) или принимает участие в распределенной атаке такого типа, направленной на другие системы и ресурсы.

Пример: отправка большого количества HTTP-запросов для создания чрезмерной нагрузки на удаленные серверы.

Загрузчики вредоносного ПО

Код, который сам по себе безвреден, но скачивает другие потенциально опасные приложения.

Код может быть загрузчиком вредоносного ПО, если выполняется хотя бы одно из условий:

- есть основания считать, что он создан для распространения потенциально опасных приложений, скачивает такие приложения или содержит код, который может скачивать и устанавливать приложения;
- как минимум 5 % приложений, скачанных этим кодом, являются потенциально опасными (то есть при минимальном пороге в 500 скачанных приложений должно быть обнаружено хотя бы 25 потенциально опасных).

Ведущие браузеры и приложения для обмена файлами не считаются загрузчиками вредоносного ПО, если:

- скачивание в них не запускается без участия пользователя;
- скачивание потенциально опасных приложений начинается только после того, как пользователь дает на это согласие.

Угроза для устройств не на базе Android

Код, потенциально опасный для других платформ.

Приложения с таким кодом безопасны для устройств Android и их пользователей, но содержат компоненты, которые могут нанести вред другим платформам.

Фишинг

Код, полученный якобы из надежного источника, который запрашивает учетные или платежные данные пользователя, а затем передает их третьим лицам. К этой же категории относится код, который перехватывает учетные данные при их передаче.

Обычно фишингу подвергаются номера кредитных карт, а также учетные данные для аккаунтов в банковских системах, играх и социальных сетях.

Повышение привилегий

Код, который нарушает целостность системы, проникая в тестовую среду, получая более высокий уровень привилегий или изменяя или отключая доступ к основным функциям, связанным с безопасностью.

Примеры:

- Приложения, которые нарушают модель разрешений Android или крадут учетные данные (такие как токены OAuth) из других приложений.
- Приложения, которые препятствуют удалению или остановке функций.
- Приложения, которые отключают модуль SELinux.

Приложения, которые без разрешения пользователя получают root-доступ через повышение привилегий, относятся к категории "Получение root-доступа".

Программы-вымогатели

Код, который получает полный или частичный контроль над устройством или данными на нем и требует, чтобы для восстановления доступа пользователь заплатил деньги или выполнил какое-либо действие.

Некоторые из таких программ шифруют данные на устройстве и требуют деньги за их расшифровку и/или получают полномочия администратора, что не позволяет пользователю удалить программу-вымогатель. Примеры:

- Программы, которые блокируют пользователю доступ к устройству и требуют деньги за его восстановление.
- Программы, которые шифруют данные и требуют плату якобы за их расшифровку.
- Программы, которые получают доступ к менеджеру правил устройства, из-за чего пользователь не может удалить эти программы.

Код, распространяемый вместе с устройством, предназначенный в первую очередь для привилегированного управления устройством, может быть исключен из категории программ-вымогателей, если он соответствует требованиям к безопасности блокировки и управления, а также к раскрытию информации и получению согласия пользователей.

Получение root-доступа

Код, который получает root-доступ к устройству.

Такой код не всегда является вредоносным. К примеру, некоторые приложения заранее предупреждают пользователя о том, что получат root-доступ к устройству, и не выполняют других опасных действий, характерных для потенциально опасных приложений.

Вредоносные приложения не уведомляют пользователя о том, что они получат root-доступ к устройству, или уведомляют, но также выполняют другие действия, характерные для потенциально опасных приложений.

Спам

Код, который отправляет незапрашиваемые сообщения контактам пользователя или использует устройство в качестве ретранслятора писем со спамом.

Шпионское ПО

Шпионским ПО называют вредоносное приложение, код или действия, которые позволяют собирать, раскрывать или передавать третьим лицам данные пользователя или устройства, не связанные с функциями, соответствующими правилам.

К шпионскому ПО также относится вредоносный код или поведение, которые могут считаться способами слежки за пользователем или приводят к раскрытию данных без его согласия или уведомления.

Шпионские действия включают, помимо прочего:

- запись аудио или вызовов на телефоне;
- кражу данных приложений;
- передачу данных с устройства, которая совершается неожиданным для пользователя способом, без его согласия или уведомления и выполняется вредоносным сторонним кодом (например, SDK) в составе приложения.

Приложения также должны соответствовать всем Правилам программы для разработчиков приложений в Google Play, в том числе связанным с данными пользователей и устройств, таким как правила в отношении нежелательного ПО для мобильных устройств, пользовательских данных и разрешений и API с доступом к конфиденциальной информации, а также требованиям к SDK.

Троянские приложения

Код, который кажется безвредным (например, обычной игрой), но выполняет нежелательные действия по отношению к пользователю.

Эта классификация обычно используется в сочетании с другими категориями потенциально опасных приложений. Троянское приложение выглядит безвредно, но содержит скрытый вредоносный компонент. Например, игра, которая в фоновом режиме отправляет платные SMS с устройства без ведома пользователя.

Примечание о необычных приложениях

Google Play Защита может посчитать новые и редкие приложения необычными при отсутствии достаточного количества данных, указывающих на безопасность. Это не означает, что приложение является вредоносным. Но в число безопасных оно сможет попасть только после дополнительной проверки.

Примечание к категории "Бэкдоры"

Включение кода в категорию бэкдоров зависит от того, что именно он делает. Чтобы код считался бэкдором, он должен позволять запускать процессы, из-за автоматического выполнения которых код попадет в другую категорию вредоносного ПО. Например, если в приложении разрешена динамическая загрузка кода и динамически загружаемый код извлекает SMS, такое приложение будет считаться бэкдором.

Но если в приложении разрешено выполнение произвольного кода и у нас нет оснований считать, что этот код добавлен для выполнения вредоносных процессов, такое приложение не будет отнесено к бэкдорам. Вместо этого мы отметим, что оно имеет уязвимость, и попросим разработчика устранить ее.

Потенциально опасное ПО

Приложения и игры, в которых функции отличаются от заявленных и скрываются различными способами. Подобные продукты кажутся безопасными пользователям и магазинам приложений, поскольку разработчики скрывают потенциально опасный контент, маскируя его, используя обфускацию и подгружая код динамически.

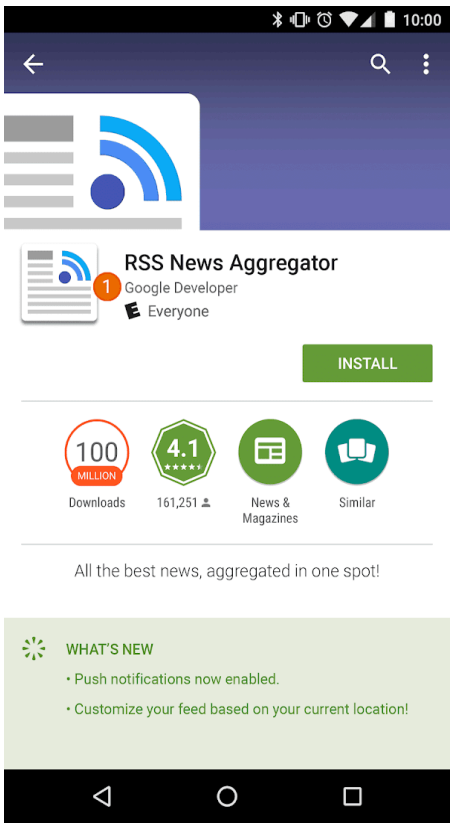
Потенциально опасное ПО похоже на другие программы из той же категории, в особенности на трояны. Однако оно скрывает вредоносное содержимое иными способами.

Выдача себя за другое лицо

Запрещены приложения, которые вводят в заблуждение пользователей, выдавая себя за другое лицо (например, другого разработчика, компанию или организацию) или другое приложение, хотя по факту не имеют к ним отношения. Не используйте значки, описания, названия и другие элементы, из-за которых пользователи могут ошибочно считать, что ваше приложение связано с другим лицом или приложением.

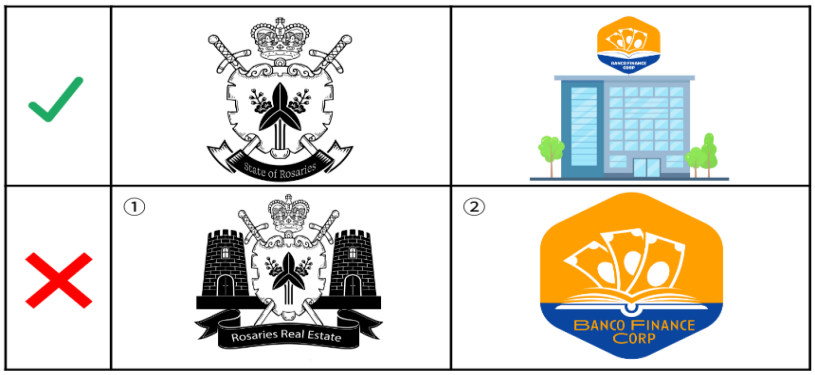
Вот примеры наиболее распространенных нарушений:

- Разработчик вводит пользователя в заблуждение относительно связи с другой компанией/разработчиком:



① Название компании-разработчика этого приложения предполагает официальную связь с Google, хотя это неправда.

- Значки и названия приложений вводят пользователя в заблуждение относительно связи с другой компанией/разработчиком:



① В приложении используется государственный герб, что создает ложное представление о том, что оно связано с органами государственной власти.
② В приложении встречается логотип организации, из-за чего пользователи ошибочно считают, что это официальное приложение компании.

- Названия и значки приложений похожи на названия и значки других продуктов или сервисов до степени смешения:

① В значке приложения используется логотип популярного сайта, связанного с криптовалютой, в результате чего возникает ложное представление о том, что это официальный сайт.
② В значке приложения встречается название и герой известного сериала, из-за чего пользователи ошибочно полагают, что оно связано с этим телешоу.

- Приложения ложно представлены как официальные от имени другой компании или лица. Запрещается использовать такие названия, как "От Димы Билана", "Официально от Димы Билана" и подобные, без соответствующих прав.
- Приложения нарушают правила фирменного оформления Android .

Ответы на часто задаваемые вопросы о правилах в отношении выдачи себя за другое лицо вы найдете в этой статье Справочного центра.

Нежелательное ПО для мобильных устройств

В Google мы прежде всего обращаем внимание на то, что нужно пользователю. В Принципах в отношении ПО и Правилах в отношении нежелательного ПО содержатся общие рекомендации для ПО, обеспечивающие удобство для пользователей. Эти правила основаны на Правилах Google в отношении нежелательного ПО и подчеркивают принципы экосистемы Android и Google Play Маркета. Программное обеспечение, которое нарушает эти принципы, потенциально опасно для пользователей. Мы стараемся защищать их от подобных программ.

В Правилах в отношении нежелательного ПО отмечено, что нежелательные программы в основном имеют следующие характеристики:

- Они не соответствуют описанию, чем вводят пользователей в заблуждение.
- Они устанавливаются обманным путем (самостоятельно или вместе с другими программами).
- Они не сообщают пользователю о своих важных функциях.
- Они вносят неожиданные изменения в систему.
- Они собирают или передают конфиденциальную информацию без ведома пользователя.
- Они собирают или передают конфиденциальную информацию небезопасным способом (например, не по протоколу HTTPS).
- Они устанавливаются в комплекте с другими программами без ведома пользователя.

На мобильных устройствах программное обеспечение представляет собой код в форме приложения, двоичного файла, модификации фреймворка и т. д. Чтобы предотвратить вред, наносимый таким ПО, и избежать сбоев в работе системы, мы предпринимаем необходимые меры.

Правила в отношении нежелательного ПО распространяются и на ПО для мобильных устройств. Мы будем расширять их по мере появления новых видов злоупотреблений.

Понятная функциональность и явное раскрытие информации

Любой код должен исполнять всё, что обещано пользователю. Приложения должны выполнять все заявленные функции и не должны вводить пользователей в заблуждение.

- Функции и цели приложения должны быть понятны.
- Явным образом объясните пользователям, какие изменения в систему будет вносить приложение. Разрешите пользователям просматривать и утверждать все важные параметры при установке.
- Программное обеспечение не должно искажать информацию о состоянии устройства, например заявлять, что система находится в критическом состоянии или заражена вирусами.
- Не используйте нелегальные методы для увеличения рекламного трафика и/или конверсии.
- Запрещены приложения, которые вводят в заблуждение пользователей, выдавая себя за другое лицо (например, другого разработчика, компанию или организацию) или другое приложение, хотя по факту не имеют к ним отношения.

Примеры нарушений:

- мошенничество с рекламой;
- социальная инженерия.

Защита пользовательских данных и конфиденциальности

Понятно и подробно расскажите о том, как приложение получает доступ к личным и конфиденциальным данным пользователя, как оно их собирает, использует и передает. При работе с ними необходимо соблюдать все действующие правила в отношении пользовательских данных, а также принимать меры предосторожности для защиты этой информации.

Приложения должны соответствовать всем Правилам программы для разработчиков приложений в Google Play, в том числе связанным с данными пользователей и устройств, таким как правила в отношении пользовательских данных, разрешений и API с доступом к конфиденциальной информации и шпионского ПО, а также требованиям к SDK.

- Не просите пользователей отключить средства защиты устройства, в том числе Google Play Защиту, и не пытайтесь обманным путем вынудить их это сделать. Например, нельзя предлагать в приложении дополнительные возможности или награды в обмен на отключение Google Play Защиты.

Обеспечение удобства пользователя

Взаимодействие с приложением должно быть простым и интуитивно понятным. Приложение должно соответствовать заявленным целям и не вводить пользователя в заблуждение.

- Если в приложении показывается реклама, она не должна нарушать функциональность устройства и появляться вне среды приложения. У пользователя должна быть возможность дать согласие на ее показ. Кроме того, ее должно быть легко отключить.
- Приложения не должны влиять на приложения других разработчиков, а также на работу устройства.
- Процесс удаления приложения должен быть простым и понятным.
- Мобильные приложения не должны имитировать уведомления операционной системы и других программ. Не отключайте предупреждения других приложений или операционной системы, особенно те, которые информируют пользователя об изменениях в ОС.

Примеры нарушений:

- объявления, прерывающие работу приложения;
- несанкционированное использование или имитация функций системы.

Загрузчики вредоносного ПО

Код, который сам по себе не является нежелательным ПО, но скачивает другое потенциально опасное ПО на мобильное устройство.

Код может быть загрузчиком вредоносного ПО, если выполняется любое из этих условий:

- есть основания полагать, что код создан, чтобы распространять нежелательное ПО, и он уже скачивал такое ПО или содержит код, который может скачивать и устанавливать приложения;
- минимум 5 % скачиваемых таким кодом приложений являются нежелательным ПО с минимальным порогом в 500 фактических скачиваний (25 фактических скачиваний нежелательного ПО).

Ведущие браузеры и приложения для обмена файлами не считаются загрузчиками вредоносного ПО, если выполняются оба условия:

- скачивание не запускается без участия пользователя;
- скачивание любого ПО начинается только после того, как пользователь даст согласие.

Мошенничество с рекламой

Мошеннические действия с рекламными объявлениями строго запрещены. Объявления, которые создают для рекламной сети видимость, будто увеличение посещаемости связано с реальным интересом пользователей – пример мошеннической рекламы и недействительного трафика. К мошенничеству с рекламой могут относиться ситуации, когда разработчики размещают рекламу запрещенными способами, например показывают скрытые объявления, используют автоматическое нажатие на объявления, изменяют информацию или прибегают к иным ручным и автоматическим (роботам, ботам и т. д.) методам генерации недействительного рекламного трафика. Недействительный трафик и мошенничество с объявлениями вредны для рекламодателей, разработчиков и пользователей и в долгосрочной перспективе снижают доверие к экосистеме мобильных объявлений.

Вот примеры наиболее распространенных нарушений:

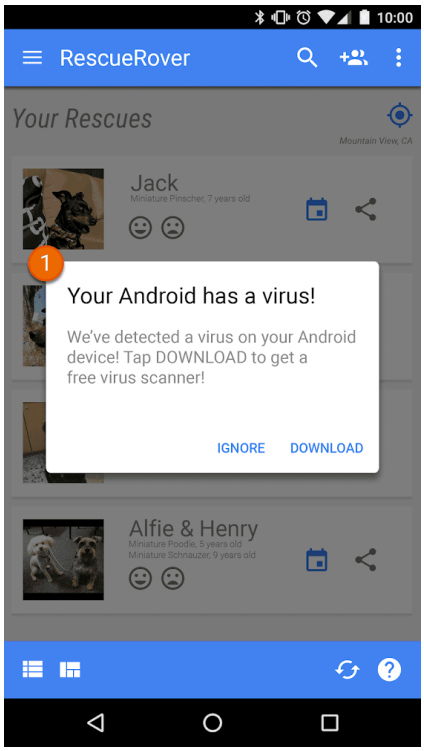
- Приложение, показывающее рекламу, которая не видна пользователям.
- Приложение, которое автоматически провоцирует нажатие на объявления без ведома пользователя или искусственно генерирует эквивалентный сетевой трафик для получения кликов.
- Приложение, отправляющее фальшивые ссылки на установку, чтобы получить оплату за установки, якобы выполненные не из сети отправителя.
- Приложение, которое выводит на экран устройства всплывающие объявления, когда само приложение закрыто.
- Приложение, которое предоставляет заведомо ложные сведения о рекламном инвентаре, например сообщает рекламным сетям, что оно работает на устройстве iOS, хотя фактически оно работает на устройстве Android, или неверно указывает название пакета, приносящего доход.

Несанкционированное использование или имитация функций системы

Приложения или объявления, которые содержатся в них, не должны имитировать функции или предупреждения операционной системы и других программ. Системные уведомления можно использовать только для неотъемлемых компонентов приложения. Например, приложение авиакомпании может показывать уведомления о распродажах билетов, а игра – о внутриигровых акциях.

Вот примеры наиболее распространенных нарушений:

- Приложения, использующие системные оповещения и предупреждения для рекламы:



① Системные уведомления, которые появляются в этом приложении, содержат рекламу.

Другие примеры с рекламой можно найти в правилах ее размещения.

Социальная инженерия

Запрещено публиковать приложения, выдающие себя за оригинальные, с целью обманом заставить пользователя выполнить действия, которые он совершил бы в исходном приложении.

Монетизация и реклама

Google Play поддерживает различные способы монетизации, включая платное распространение, подписку и рекламу, а также продажу контента через приложение. Чтобы обеспечить удовлетворенность пользователей, мы требуем, чтобы вы соблюдали перечисленные ниже правила.

Платежи

1. Разработчики, которые взимают средства за скачивание приложений из Google Play, должны использовать для таких транзакций платежную систему Google Play.
2. Если в приложении, распространяемом через Google Play, требуется или принимается плата за доступ к функциям или сервисам, включая любые возможности приложения, цифровой контент или товары (далее – покупки в приложении), разработчик должен использовать для таких транзакций платежную систему Google Play, за исключением случаев, указанных в разделах 3, 8 и 9.

   Примерами функций или сервисов, требующих использования платежной системы Google Play, являются в том числе следующие Покупки в приложении:

   - Объекты (например, виртуальная валюта, дополнительное время или дополнительные жизни в игре, новые предметы, персонажи и аватары).
   - Подписки (например, на игровой, образовательный, музыкальный, фитнес- или видеоконтент, расширенные версии сервисов и т. д.).
   - Функции и контент (например, версия приложения без рекламы или возможности, недоступные в бесплатной версии).
   - Облачные сервисы и программные продукты (например, хранилища данных, а также ПО для управления финансами и эффективного ведения бизнеса).

3. Платежную систему Google Play нельзя использовать в перечисленных ниже случаях.
   a. Если вы преимущественно принимаете платежи за:
      - покупку или аренду товаров (например, продуктов питания, одежды, товаров для дома и электронных устройств);
      - услуги, оказываемые в реальном мире (например, транспорт, услуги клининга, авиабилет, абонемент в тренажерный зал, доставка еды, билеты на концерт);
      - оплату счетов по кредитной карте или счетов за коммунальные услуги (например, кабельное телевидение и телекоммуникационные услуги).

   b. При переводе средств другим пользователям, сборе пожертвований, не облагаемых налогами, и оплате покупок на онлайн-аукционах.
   c. При оплате контента или сервисов, которые помогают участвовать в азартных онлайн-играх, согласно разделу Приложения для азартных игр Правил в отношении азартных игр, игр и соревнований с реальными денежными призами.
   d. При оплате покупок из категорий товаров, которые считаются неприемлемыми согласно правилам платежного центра в отношении контента .

      Примечание. На некоторых рынках мы разрешаем использовать Google Pay в приложениях, предназначенных для продажи физических товаров и/или услуг. Подробная информация приведена

на странице Google Pay для разработчиков .

4. Предлагать в приложениях другие способы оплаты, кроме платежной системы Google Play, запрещено (за исключением случаев, описанных в разделах 3, 8 и 9). В частности, пользователям нельзя предлагать другие способы оплаты:
   - на странице приложения в Google Play;
   - в рекламе внутри приложения, касающейся платного контента;
   - в компонентах WebView, кнопках, ссылках, сообщениях, рекламе и других призывах к действию внутри приложения;
   - в пользовательском интерфейсе, в том числе на экранах регистрации и создания аккаунта: ни в одном их разделе пользователей нельзя перенаправлять к способу оплаты, отличному от платежной системы Google Play.
5. Виртуальная валюта внутри приложений должна использоваться только в том продукте, в котором она была куплена.
6. Разработчики обязаны явно и четко информировать пользователей об условиях и ценах на приложение или любые функции и подписки. Цены внутри приложения должны совпадать с ценами, которые появляются в платежном интерфейсе Google Play. Если за доступ к функциям, упомянутым в описании приложения в Google Play, взимается отдельная или дополнительная плата, вы обязаны предупредить об этом пользователей на странице приложения.
7. Если в приложении или игре есть механизмы, позволяющие в результате покупки получить случайные виртуальные предметы (включая, помимо прочего, лутбоксы), то вы должны своевременно и непосредственно перед покупкой явным образом сообщить пользователю, какова вероятность получить такие предметы.
8. За исключением случаев, указанных в разделе 3, разработчики распространяемых через Google Play приложений, в которых от пользователей в указанных странах и регионах требуется или принимается плата за Покупки в приложениях, могут предлагать внутри приложений альтернативную платежную систему в дополнение к системе Google Play. Для этого необходимо заполнить форму декларации для подходящей программы и принять дополнительные условия и требования программы, указанные в этой форме.
9. Разработчики распространяемых через Google Play приложений могут предлагать пользователям из стран Европейской экономической зоны (ЕЭЗ) переходить в другие приложения и на другие сайты, например для продвижения цифровых специальных функций и услуг в приложении. Такие разработчики должны заполнить форму декларации для программы и принять дополнительные условия и требования программы, указанные в этой форме.

Примечание. Чтобы узнать сроки и получить ответы на часто задаваемые вопросы по этим правилам, посетите Справочный центр.

Реклама

Для поддержания качества мы учитываем содержание, аудиторию и способ показа объявления, а также удобство, безопасность и конфиденциальность пользователей. Объявления и связанные с ними специальные предложения считаются частью приложения, поэтому должны соответствовать всем правилам Google Play. Если вы монетизируете в Google Play приложение, предназначенное для детей, то на рекламу в нем распространяются дополнительные требования.

В Справочном центре можно узнать больше о правилах в отношении продвижения и данных для Google Play, а также о нарушениях, связанных с методами продвижения, которые вводят пользователей в заблуждение.

Содержание объявления

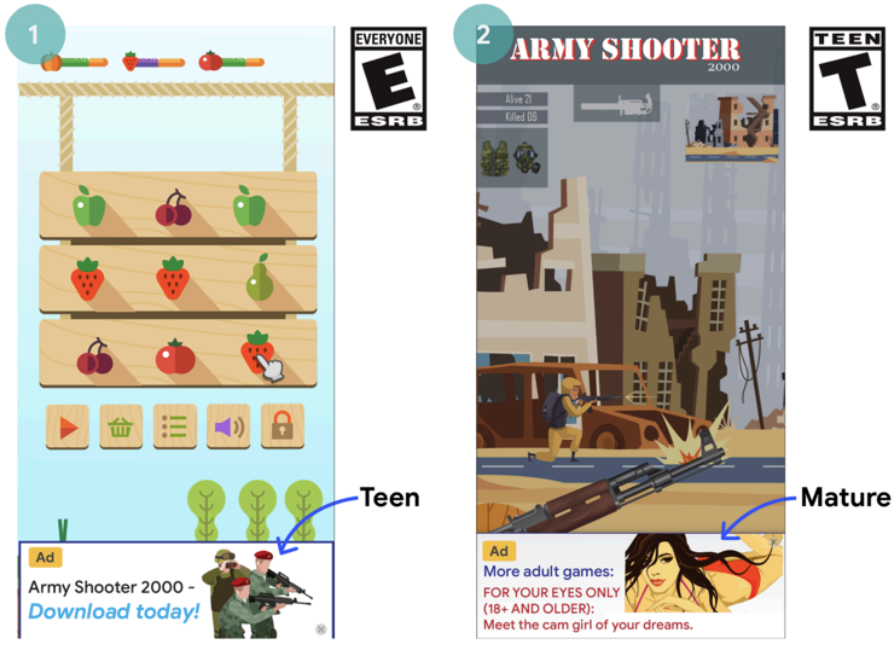
Объявления и связанные с ними специальные предложения считаются частью приложения и должны соответствовать нашим правилам в отношении запрещенного контента. На приложения для азартных игр распространяются дополнительные требования.

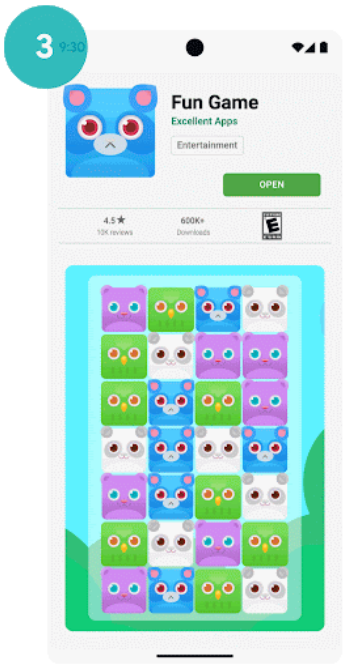
Неприемлемые объявления

Как контент приложения, так и показываемые в нем объявления и связанные с ними предложения (например, когда реклама предлагает скачать другое приложение), необходимо подбирать с учетом возрастных ограничений приложения.

Вот примеры наиболее распространенных нарушений:

- Объявления, которые не соответствуют возрастным ограничениям приложения:





① Объявление неприемлемо для целевой аудитории приложения (Для всех), поскольку предназначено для подростков.
② Объявление неприемлемо для целевой аудитории приложения (Подростки), поскольку предназначено для взрослых.

③ Объявление с предложением скачать приложение для взрослых неприемлемо для целевой аудитории игры (Для всех).

Требования к объявлениям в приложениях для всей семьи

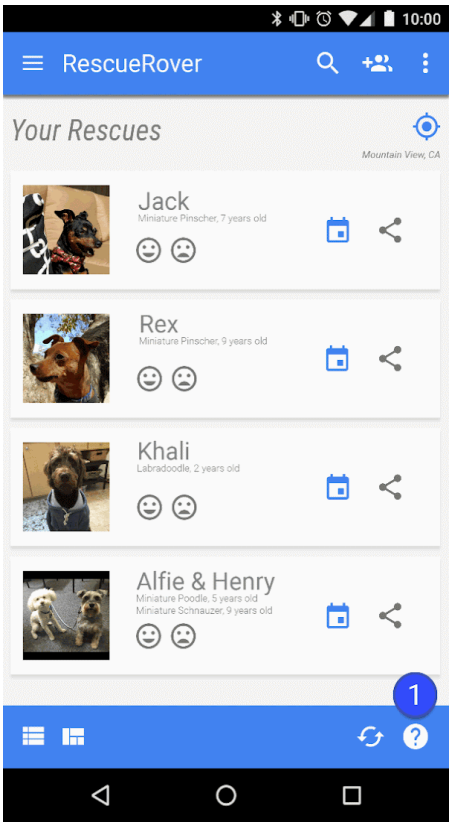
Если вы монетизируете в Google Play приложение, предназначенное для детей, оно должно соответствовать требованиям программы "Приложения для всей семьи" в отношении рекламы и монетизации.

Объявления, вводящие в заблуждение

В объявлениях нельзя копировать элементы интерфейса приложения, в том числе уведомления и системные предупреждения. Пользователю должно быть понятно, в каком именно приложении появляется объявление.

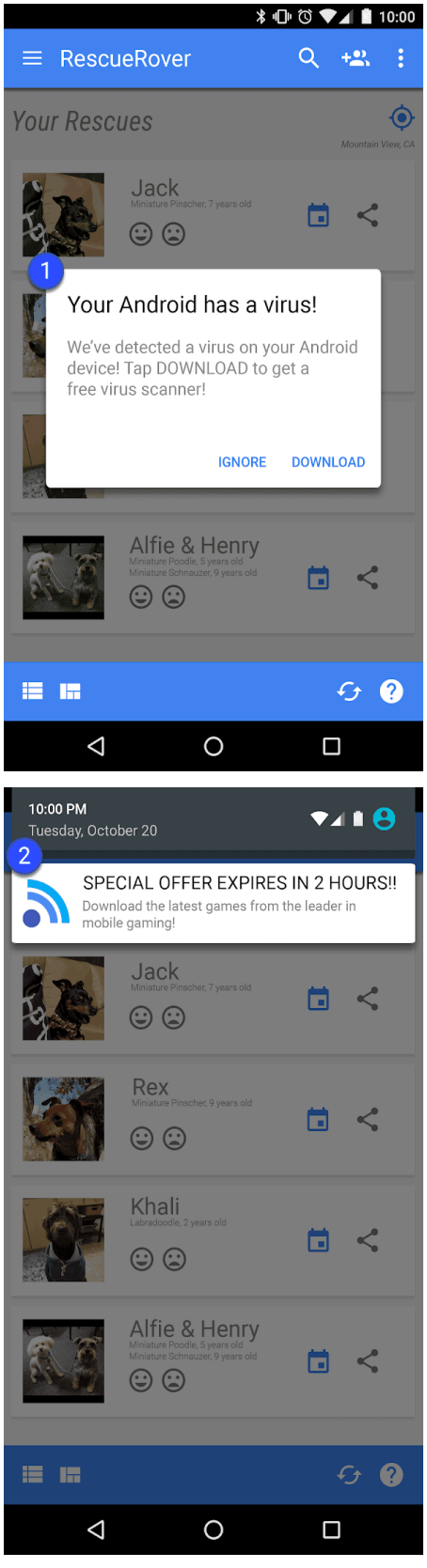
Вот примеры наиболее распространенных нарушений:

- Объявления, которые выглядят, как интерфейс приложения:

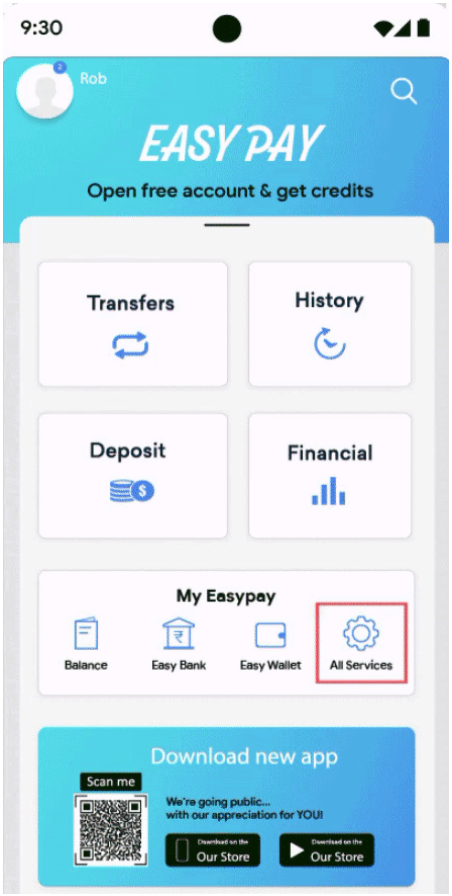


① В этом приложении вопросительный знак на самом деле является объявлением, которое перенаправляет пользователя на внешнюю целевую страницу.

- Объявления, которые копируют системные оповещения:



① ② Выше представлены примеры объявлений, которые внешне похожи на системные уведомления.



① Выше представлен пример раздела, элементы которого похожи на список функций, но перенаправляют пользователя на рекламу.

Объявления, прерывающие работу приложения

Объявления, прерывающие работу приложения, появляются в неожиданных местах, могут приводить к непреднамеренным нажатиям и нарушать функциональность устройства.

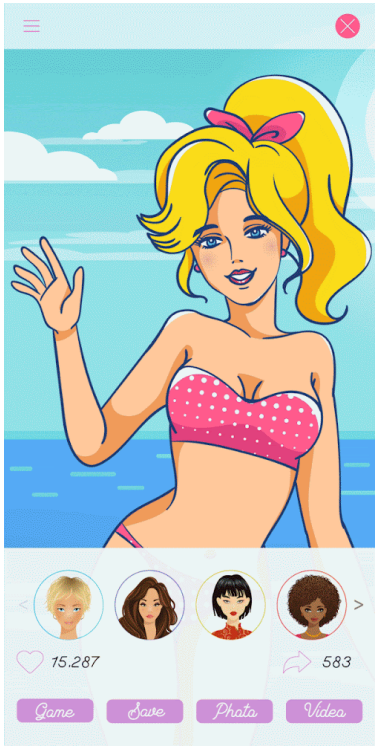
Нельзя вынуждать пользователя нажимать на объявление или отправлять личные данные для рекламных целей, прежде чем он получит полный доступ к приложению. Объявления не должны показываться вне приложения или влиять на другие приложения и рекламу в них, а также на работу устройства, его портов и системных или физических кнопок. В частности, это относится к оверлеям, сопутствующим функциям и рекламным блокам – виджетам. Если в приложении есть объявления, которые не позволяют нормально его использовать, они должны легко закрываться.

Вот примеры наиболее распространенных нарушений:

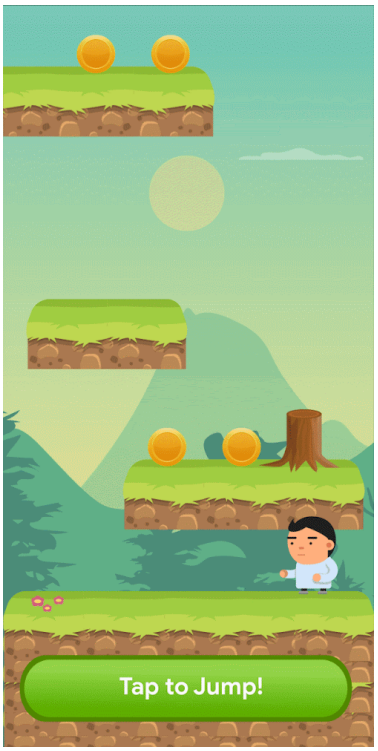
- Реклама, которая занимает весь экран, не позволяет нормально использовать приложение и не закрывается явным способом:

① В этом объявлении нет кнопки "Закрыть".

- Реклама, вынуждающая пользователя переходить по ссылкам с помощью ложной кнопки "Закрыть" или внезапного появления в тех частях экрана, на которые обычно нажимают для доступа к другим функциям приложения:

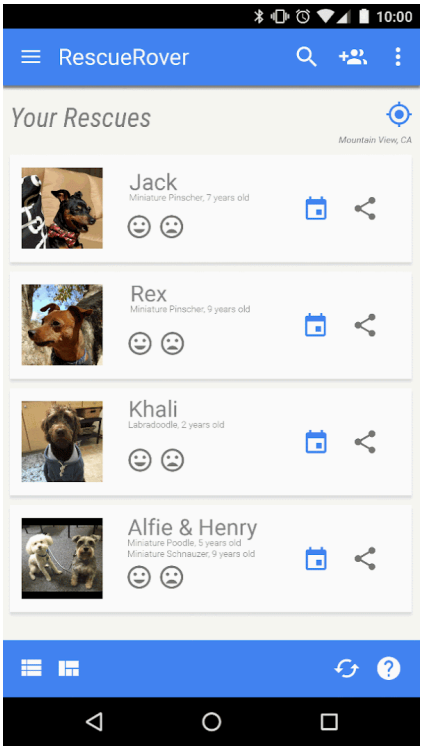


① В этом объявлении используется ложная кнопка "Закрыть".



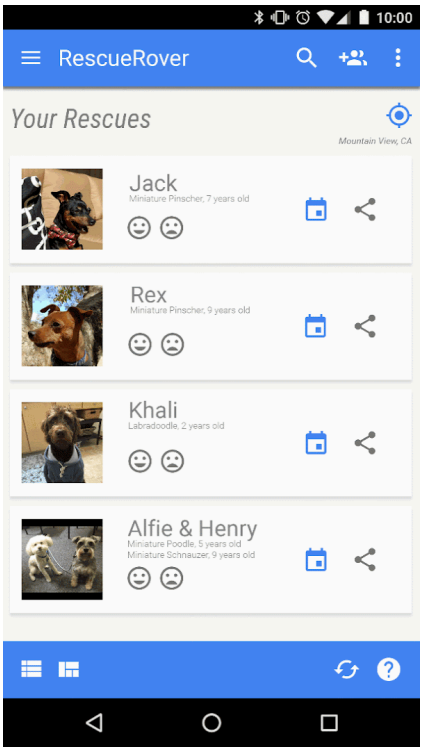
② Это объявление внезапно появляется в той части экрана, на которую пользователь привык нажимать для доступа к функциям приложения.

- Реклама в приложении, которая показывается вне его:



① Пользователь переходит из этого приложения на главный экран, где внезапно появляется реклама.

- Реклама, которая появляется после нажатия кнопки главного экрана или выполнения других действий, предназначенных для выхода из приложения:



① Пользователь пытается закрыть приложение и перейти на главный экран, но этот процесс прерывается рекламой.

Более качественная реклама

Чтобы использование приложений Google Play было максимально комфортным, разработчики должны соблюдать следующие рекомендации по размещению рекламы. Если пользователи не ожидают этого, запрещается показывать:

- полноэкранные межстраничные объявления любого формата (видео, GIF, статические изображения и пр.), которые появляются неожиданно, обычно когда пользователь выполняет действие, не связанное с темой объявления;
  - объявления во время игры в начале уровня или при показе очередного блока контента;
  - межстраничные объявления в формате полноэкранного видео, которые появляются до экрана загрузки приложения (заставки);
- полноэкранные межстраничные объявления любого формата, которые невозможно закрыть по истечении 15 сек. Полноэкранные межстраничные объявления, которые разрешены пользователем или не мешают выполнять действия (например, при показе после страницы с результатами игры), могут показываться дольше 15 сек.

Эти правила не применяются к объявлениям с вознаграждением, которые явно разрешены пользователем (например, если разработчик предлагает посмотреть рекламу в обмен на разблокировку игровой функции или контента). Эти правила также не действуют в отношении монетизации и рекламы, которые не мешают нормальному использованию приложения или игры (например, допускается видеоконтент со встроенными объявлениями и неполноэкранные баннеры).

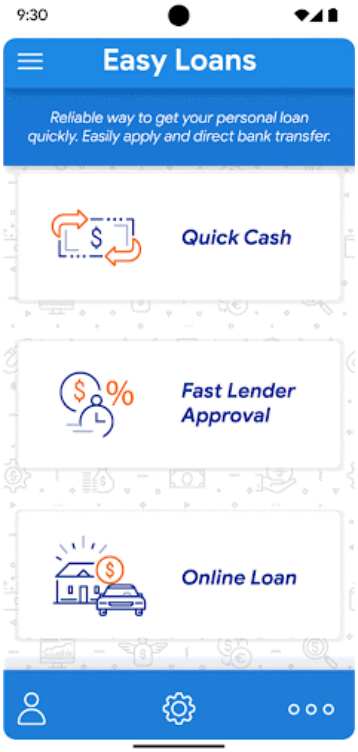
Эти рекомендации сформулированы на основе стандартов Better Ads Standards – Mobile Apps Experiences . Дополнительные сведения об этих стандартах вы найдете на сайте Coalition for Better Ads .

Вот примеры наиболее распространенных нарушений:

- Неожиданные объявления, которые показываются во время игры или перед появлением очередного блока контента (например, после того как пользователь нажал кнопку, но до выполнения связанного с ней действия). Пользователи ожидают начала игры или появления

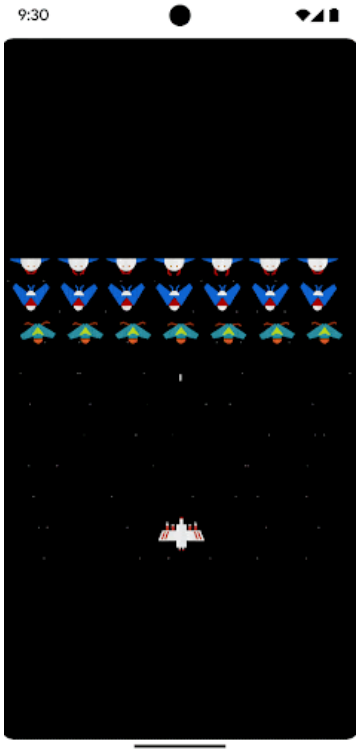
новой информации, а не показа рекламы.

① Статическое объявление неожиданно появляется во время игры в начале уровня.



② Видеореклама неожиданно появляется в начале блока контента.

- Полноэкранное объявление, которое появляется во время игры и не может быть закрыто через 15 сек.



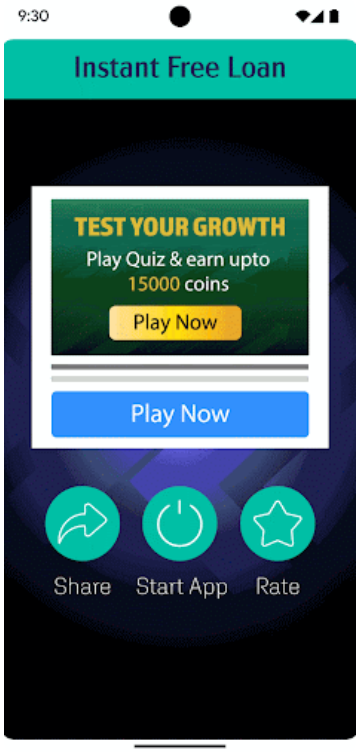
① Межстраничное объявление появляется во время игры, и его невозможно закрыть по истечении 15 сек.

Рекламные приложения

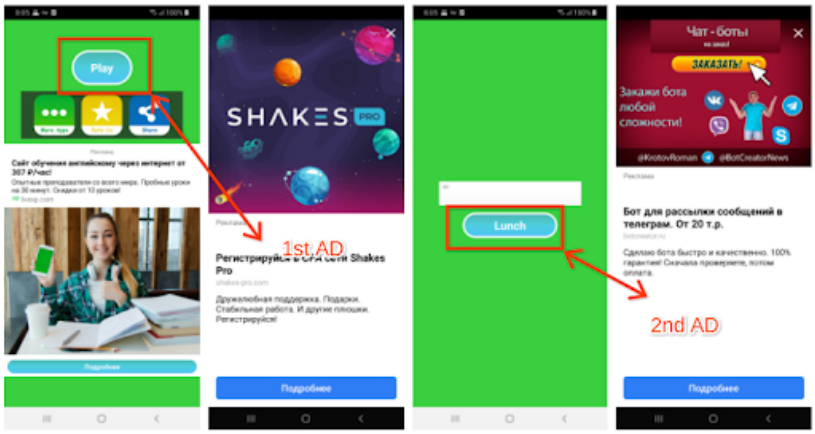
Запрещается публиковать приложения, показывающие межстраничные объявления, которые отвлекают пользователя от взаимодействия с приложением и выполнения задач в нем.

Вот примеры наиболее распространенных нарушений:

- Приложения, в которых после каждого действия пользователя (в том числе после нажатий, пролистывания и т. д.) показываются межстраничные объявления.



① На первой странице приложения располагается несколько активных кнопок. Когда пользователь нажимает кнопку **Старт**, появляется межстраничное объявление. Закрыв его, пользователь возвращается в приложение и выбирает **Сервис**, чтобы начать работу, но в этот момент открывается другое объявление.



② На первой странице приложения активна только кнопка **Играть**. После нажатия на нее появляется межстраничное объявление. Закрыв его, пользователь выбирает **Старт**, так как это единственная активная кнопка, и в этот момент открывается другое объявление.

Монетизация функций блокировки экрана

Запрещено показывать рекламу и размещать платные функции на заблокированном экране, кроме тех случаев, когда приложение предназначено исключительно для управления заблокированным экраном.

Мошенничество с рекламой

Мошеннические действия с объявлениями строго запрещены. Дополнительную информацию вы найдете в наших правилах в отношении мошенничества с рекламой.

Использование данных о местоположении в целях рекламы

Приложения, которые используют доступ к данным о местоположении устройства для показа рекламы, должны соответствовать положениям раздела Личная и конфиденциальная информация, а также следующим требованиям:

- Нужно ясно донести до пользователя, что если он предоставит разрешение, то данные о местоположении его устройства будут собираться или использоваться для показа рекламы. Вы должны сообщить об этом в обязательной политике конфиденциальности приложения, а также добавить ссылки на политики конфиденциальности рекламных сетей в отношении использования данных о местоположении.
- Разрешения на доступ к данным о местоположении могут запрашиваться только для работы функций и сервисов, которые есть в приложении. Нельзя запрашивать доступ к данным о местоположении, если он будет использоваться только для рекламы.

Использование рекламного идентификатора Android

В сервисах Google Play 4.0 появились новые API, а также идентификатор для рекламодателей и тех, кто предоставляет услуги аналитики. Условия использования идентификатора приведены ниже.

- **Использование.** Рекламный идентификатор Android (AAID) должен использоваться только для размещения рекламы и анализа ее показателей. При каждом обращении к идентификатору должны проверяться значения параметров "Реклама на основе интересов" и "Персонализация рекламы".

- **Связь с информацией, позволяющей идентифицировать личность, и другими идентификаторами.**
  - Рекламный идентификатор нельзя связывать с постоянными идентификаторами устройства, такими как SSAID, MAC-адрес или IMEI-код, в рекламных целях. Рекламный идентификатор можно связывать с данными, позволяющими идентифицировать личность, только при наличии явного согласия пользователя.
  - Запрещается связывать в аналитических целях рекламный идентификатор с данными, позволяющими идентифицировать личность, или постоянными идентификаторами устройства, такими как SSAID, MAC-адрес или IMEI-код. Подробная информация о постоянных идентификаторах устройства приведена в правилах в отношении пользовательских данных .
- **Уважение предпочтений пользователя.**
  - Новый рекламный идентификатор, присвоенный после сброса, никоим образом не должен быть связан с предыдущим идентификатором или его данными без явно выраженного согласия пользователя.
  - Кроме того, необходимо учитывать настройки пользователя в отношении подбора и персонализации рекламы. Если эти функции отключены, то вам запрещается использовать рекламный идентификатор для создания пользовательского профиля в рекламных целях или для показа персонализированных объявлений. К разрешенным методам относятся контекстная реклама, ограничение частоты показов, отслеживание конверсий, сообщения о нарушениях, а также обнаружение угроз безопасности и случаев мошенничества.
  - Если рекламный идентификатор Android удаляется на новом устройстве, он становится недоступен. Вместо него будет показываться строка, состоящая из нулей. Устройство без рекламного идентификатора нельзя связывать с данными предыдущего идентификатора.
- **Уведомление пользователей.** В примечании о конфиденциальности, соответствующем требованиям законодательства, пользователю необходимо сообщить о сборе и использовании рекламных идентификаторов, а также о настоящих правилах. Подробная информация о наших стандартах конфиденциальности приведена в разделе Данные пользователя .
- **Соблюдение условий использования.** Рекламный идентификатор можно применять только в соответствии с Правилами программы для разработчиков приложений в Google Play, причем это условие распространяется на всех, кому вы можете предоставить идентификатор в ходе коммерческой деятельности. В любом приложении, загружаемом или публикуемом в Google Play, следует использовать рекламный идентификатор (если он доступен на устройстве). Применять для рекламных целей другие идентификаторы устройств запрещено.

Дополнительная информация представлена в наших правилах в отношении пользовательских данных.

Подписки

Разработчикам запрещено вводить пользователей в заблуждение относительно сервисов и контента, доступных по подписке. Информация о ней, в том числе на заставках, экране выбора тарифного плана и в самом приложении, должна быть понятной. Мы не допускаем приложения, которые обманным или манипулятивным путем принуждают пользователей совершать покупки (в том числе приобретать подписки и контент в приложениях). Необходимо указывать только достоверные и точные сведения о преимуществах подписки и других ее аспектах.

Предложение должно содержать всю необходимую информацию, в том числе об условиях, стоимости подписки, периодичности оплаты и автоматическом продлении, а также о том, можно ли пользоваться приложением без подписки. Все эти сведения должны быть доступны без дополнительных действий со стороны пользователя.

Пользователи, которые приобрели подписку, должны получать постоянные или регулярные преимущества в течение всего срока ее действия. Например, в рамках подписки запрещено

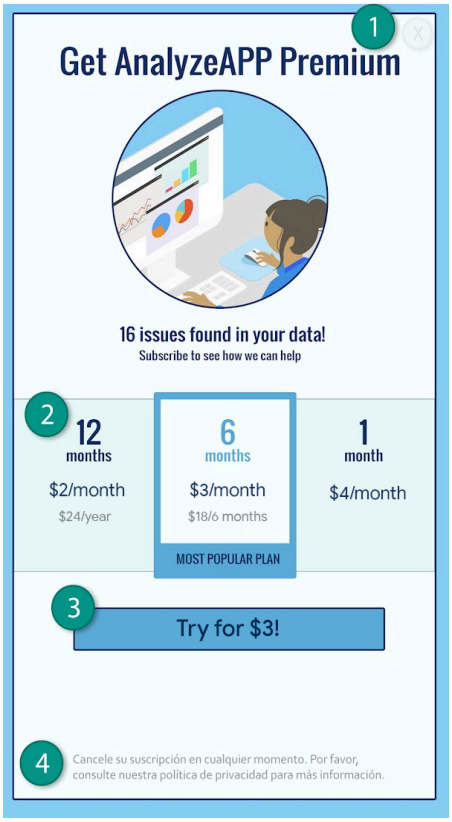
предоставлять одноразовые игровые бонусы или перечислять валюту приложения единым платежом. Вы можете предоставлять вознаграждения или бонусы только в дополнение к постоянным или регулярным преимуществам, которые действуют на протяжении срока действия подписки. Если таких преимуществ нет, вместо подписки необходимо предлагать контент для продажи через приложение.

Запрещено представлять разовое предложение как подписку. Кроме того, нельзя менять условия уже оформленной подписки (например, отменять, уменьшать количество регулярных бонусов или прекращать их поддержку) таким образом, чтобы фактически пользователи получали только однократное преимущество.

Вот примеры наиболее распространенных нарушений:

- Ежемесячные подписки, в условиях которых не указано, что они будут автоматически продляться каждый месяц со списанием средств со счета.
- Годовые подписки, в информации о которых наиболее заметно выделена их месячная стоимость.
- Неполная локализация условий и стоимости подписки.
- Предложения, в которых неясно указано, что пользователь может получить доступ к контенту без подписки (если это возможно).
- Неточное указание наименования товара, например для подписки с автоматическим списанием средств дана формулировка "Бесплатная пробная версия" или "Попробуйте подписку Premium – 3 дня бесплатно".
- Распределение процесса покупки на несколько экранов таким образом, чтобы пользователи могли случайно нажать кнопку подписки.
- Подписки, в которых нет постоянных или регулярных преимуществ. Например, 1 000 кристаллов в первый месяц подписки и 1 кристалл в каждый следующий месяц до конца ее срока действия.
- Получение разового преимущества за оформление подписки с автоматическим продлением и ее отмена после покупки без запроса со стороны пользователя.

Пример 1



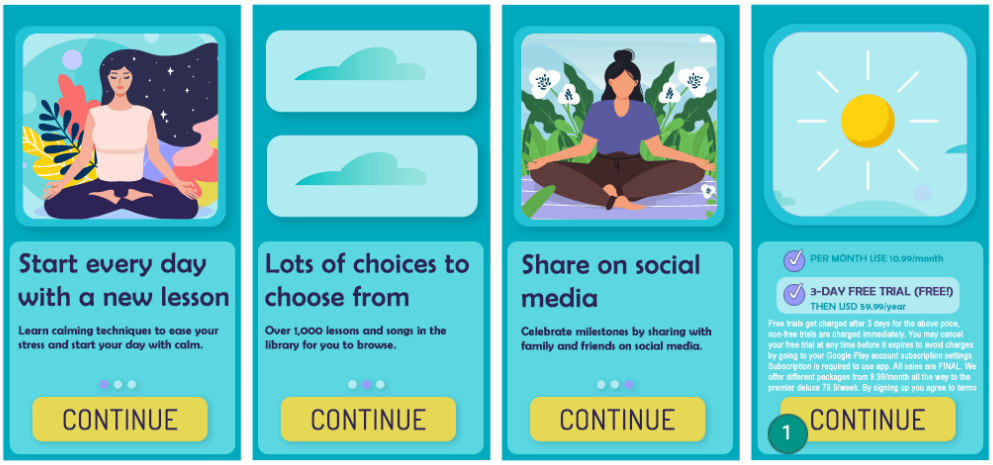
① Кнопка "Закрыть" отсутствует или плохо видна, и пользователь может не понять, что функции приложения будут доступны и без подписки.

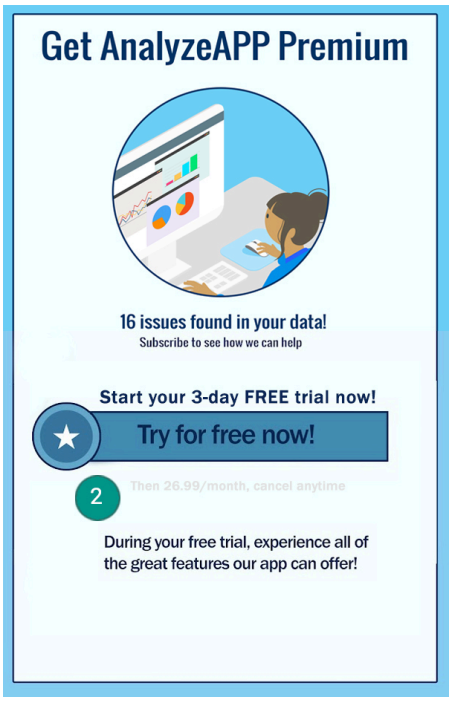
② В предложении выделяется цена за месяц, а не фактическая сумма. Пользователь может не понять, что при оформлении подписки будет списана плата за шесть месяцев.

③ В предложении указана только начальная цена, и пользователь может не понять, какая сумма будет списываться автоматически после завершения начального периода.

④ Условия использования локализованы, а текст предложения и валюта – нет, поэтому часть информации может быть непонятна.

Пример 2





① Для перехода к каждому следующему экрану нужно нажимать в одной и той же области, и при последнем нажатии кнопки "Продолжить" оформляется подписка.

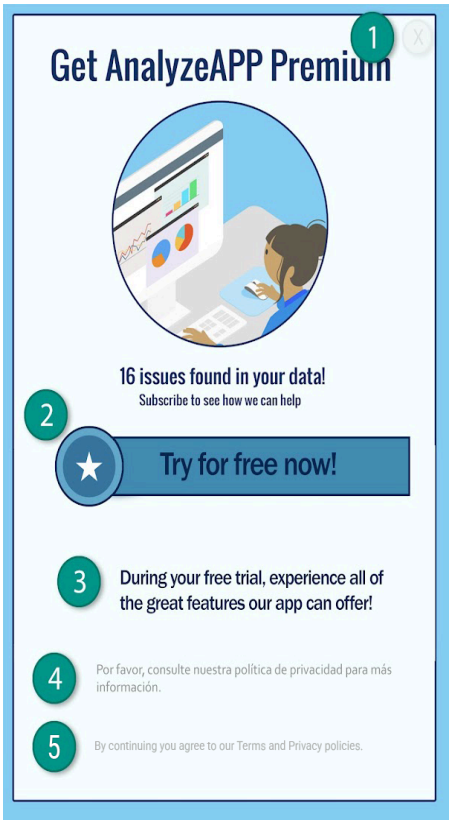
② Сумму, которую предстоит заплатить в конце пробного периода, трудно прочитать, поэтому пользователь может подумать, что это бесплатный тарифный план.

Бесплатные пробные версии и предложения для новых пользователей

Ещё до того, как пользователь оформит подписку, вы должны предоставить ему ясное и точное описание условий вашего предложения, включая продолжительность, цену, доступный контент или сервисы. Не забудьте объяснить, как и когда пользователь перейдет с бесплатной пробной версии на платную подписку, уточнить стоимость и указать способы отменить подписку до окончания пробного периода.

Вот примеры наиболее распространенных нарушений:

- Предложения, в которых не указан или неясно указан срок действия бесплатной пробной версии или цены для новых пользователей.
- Предложения, в которых четко не указано, что после окончания срока действия предложения подписка автоматически станет платной.
- Предложения, в которых четко не указано, что пользователь может получить доступ к контенту, не используя пробную версию подписки (если это возможно).
- Предложения, для которых условия и цены локализованы не полностью.



① Кнопка "Закрыть" отсутствует или плохо видна, и пользователь может не понять, что функции приложения будут доступны и без подписки.

② В предложении сделан акцент на бесплатной пробной версии, и пользователь может не понять, что в конце пробного периода автоматически начнет взиматься плата.

③ В предложении не указаны сроки пробного периода, и пользователь может не понять, как долго контент будет доступен бесплатно.

④ Условия использования локализованы, а текст предложения и валюта – нет, поэтому часть информации может быть непонятна.

⑤ В предложении не объясняется, как можно отменить бесплатную пробную подписку, чтобы после окончания ее действия не начала взиматься плата.

Управление подписками, их отмена и возврат средств

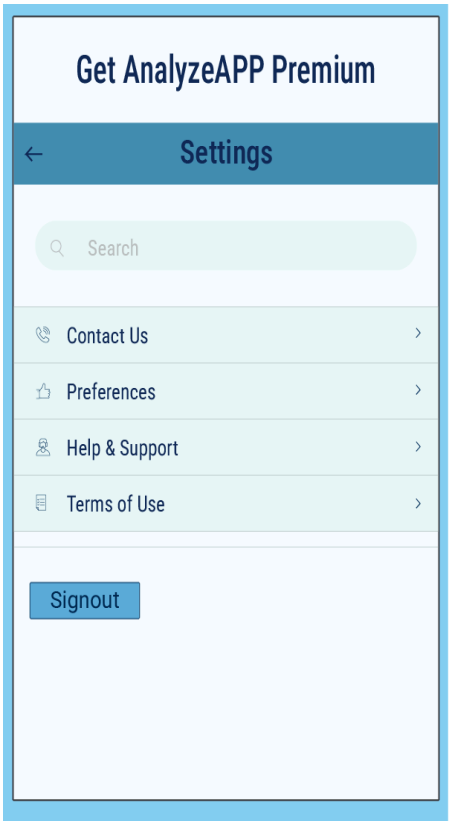
Если в вашем приложении продаются подписки, необходимо понятно объяснить, как можно отменить их или управлять ими. В приложении также должна быть возможность отмены подписки онлайн. Для этого в настройках аккаунта приложения или на аналогичной странице можно:

- указать ссылку на центр подписок Google Play (для подписок, которые продаются с использованием платежной системы Google Play);
- предоставить способ напрямую отменить подписку.

Согласно правилам Google Play при отмене подписки, купленной через платежную систему Google Play, возврат средств за текущий расчетный период не производится. При этом контент, доступный по подписке, предоставляется пользователю до конца этого периода. Затем подписка отменяется. Пользователи в некоторых странах могут отменить подписку сразу и получить возврат средств за оставшееся время согласно действующему законодательству.

В качестве поставщика контента или доступа вы можете установить более гибкие правила возврата платежей. Убедитесь, что правила подписки, ее отмены и возврата платежей соответствуют действующему законодательству, а также обязательно сообщайте пользователям обо всех изменениях в этих правилах.

Вот примеры наиболее распространенных нарушений:



В приложении, например в настройках аккаунта, нет ссылки на страницу, где можно управлять подписками и отменять их.

Программа самостоятельной сертификации рекламных SDK в приложениях для всей семьи

Как описано в правилах программы "Приложения для всей семьи" , при размещении рекламы в приложении, предназначенном только для детей, необходимо использовать исключительно рекламные SDK, которые прошли самостоятельную сертификацию на соответствие правилам Google Play, включая приведенные ниже требования к самостоятельной сертификации рекламных SDK.

Если приложение рассчитано как на детей, так и на взрослых, вы должны сделать так, чтобы дети видели только те объявления, для которых использовались рекламные SDK с самостоятельной сертификацией. Добиться этого можно, например, с помощью нейтрального возрастного фильтра.

Вы обязаны следить за тем, чтобы все используемые вами версии SDK, в том числе с самостоятельной сертификацией, соответствовали действующим правилам, законам и нормам. Компания Google не делает никаких заявлений и не дает гарантий относительно точности информации, предоставленной рекламными SDK в процессе самостоятельной сертификации.

Самостоятельная сертификация рекламных SDK в приложениях для всей семьи обязательна только в том случае, если эти SDK используются для показа рекламы детям. Вы несете ответственность за содержание объявлений и сбор сведений согласно правилам в отношении пользовательских данных и правилам программы "Приложения для всей семьи". Сертификация не требуется:

- для показа собственной рекламы, когда SDK используется для мерчандайзинга и перекрестного продвижения ваших приложений или другого вашего медиаконтента;
- для прямых сделок с рекламодателями, при которых SDK используется только для управления инвентарем.

Требования к самостоятельной сертификации рекламных SDK в приложениях для всей семьи

- Определите признаки нежелательных объявлений и запретите их в условиях или политике рекламного SDK. Определения должны соответствовать Правилам программы для разработчиков приложений в Google Play.
- Выберите способ, с помощью которого будете присваивать объявлениям возрастные ограничения. Необходимо настроить не менее двух категорий: "Для всех" и "Для взрослых". Возрастные ограничения должны присваиваться по тому же методу, который используется в сертифицированных рекламных SDK Google.
- Разрешите издателям запрашивать показ объявлений, ориентированных на детей (в определенных приложениях или в каждом конкретном случае). Убедитесь, что контент в объявлениях не нарушает действующее законодательство, например закон США "О защите личных сведений детей в интернете" (COPPA) и Генеральный регламент ЕС о защите персональных данных (GDPR). Кроме того, в рекламных SDK, которые используются в ресурсах для детей, необходимо отключить персонализированную рекламу, рекламу на основе интересов, а также ремаркетинг.
- Ограничьте выбор издателей форматами объявлений, соответствующими правилам в отношении рекламы и монетизации программы "Приложения для всей семьи", а также требованиям программы "Одобрено преподавателями".
- Если для показа рекламы детям используется технология назначения ставок в реальном времени, убедитесь, что файлы объявления проверены, а участникам аукциона присваиваются индикаторы конфиденциальности.
- Чтобы подтвердить соответствие рекламного SDK правилам, предоставьте Google тестовую версию приложения и все необходимые сведения в специальной форме. Своевременно отвечайте на последующие запросы информации. Например, отправляйте данные о новых версиях приложения вместе с тестовым приложением, чтобы подтверждать соответствие версии рекламного SDK всем требованиям к самостоятельной сертификации.
- Проходите самостоятельную сертификацию, чтобы подтверждать соответствие новых версий Правилам программы для разработчиков приложений в Google Play, в том числе правилам программы "Приложения для всей семьи".

Примечание. Рекламные SDK с самостоятельной сертификацией в приложениях для всей семьи необходимо использовать для показа объявлений в соответствии со всеми законами и положениями, связанными с детьми и потенциально применимыми к деятельности издателей.

Подробнее о водяных знаках в креативах и предоставлении тестовой версии приложения ...

Требования к платформам медиации, показывающим рекламу детям:

- Следует использовать только рекламные SDK, прошедшие самостоятельную сертификацию в рамках Программы рекламы в приложениях для всей семьи, или принимать меры, гарантирующие, что все объявления на платформах медиации будут соответствовать этим требованиям.
- Необходимо передавать информацию о рейтинге рекламного контента и о том, что ресурс предназначен для детей.

Изучите список рекламных SDK, прошедших самостоятельную сертификацию в приложениях для всей семьи, и конкретные версии таких SDK .

Если вы знаете организации, желающие самостоятельно сертифицировать рекламные SDK, вы можете отправить им форму .

Данные для Google Play и продвижение

Методы, которые вы применяете для продвижения своего приложения, значительно влияют на восприятие Google Play посетителями. Не используйте низкокачественную рекламу и спам, а также не завышайте популярность приложения искусственно.

Продвижение приложения

Запрещено публиковать приложения, прямо или косвенно связанные с методами продвижения, которые вводят в заблуждение или иным образом причиняют вред пользователям, а также сообществу разработчиков. Считается, что методы вводят в заблуждение и причиняют вред, если они нарушают Правила программы для разработчиков.

Вот примеры наиболее распространенных нарушений:

- Показ рекламы, вводящей в заблуждение , в приложениях, на сайтах и других ресурсах. Например, к ней относятся объявления, похожие на системные уведомления.
- Показ рекламы сексуального характера для перенаправления пользователей на страницу приложения в Google Play.
- Продвижение и установка, в результате которых происходит перенаправление пользователей в Google Play или скачивание приложения без предварительного запроса.
- Продвижение с помощью нежелательных SMS-рассылок.
- Добавление в имя разработчика, название или значок приложения текста или изображений со сведениями о рейтинге или об успехе приложения в Google Play, ценами и рекламой, а также информацией об участии в существующих программах Google Play.

Вы обязаны следить за тем, чтобы эти правила соблюдались в рекламных сетях, партнерских программах и объявлениях, связанных с вашим приложением.

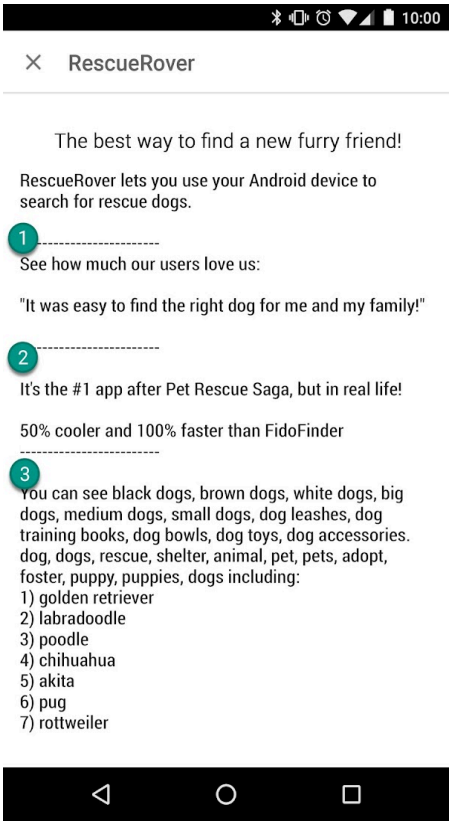
Метаданные

Из описания приложения пользователи узнают о его функциях и назначении. Мы запрещаем публиковать приложения с ложными, неправильно отформатированными, недостаточными, нерелевантными, излишними или недопустимыми метаданными. К метаданным, помимо прочего, относятся название и описание приложения, его значок, скриншоты и рекламные изображения, а также название компании-разработчика. Описание приложения должно быть понятным и грамотным. Мы также запрещаем включать в описание отзывы пользователей без указания автора цитаты.

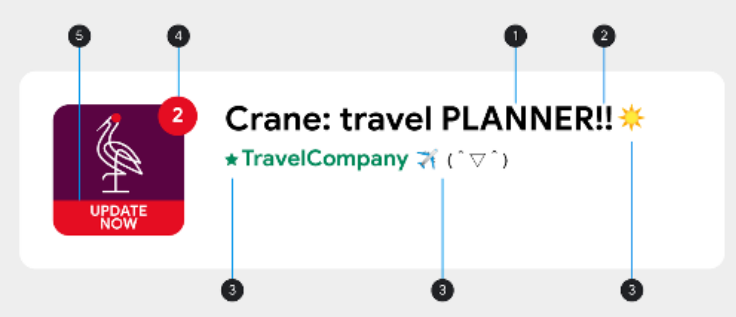
Название и значок приложения, а также название компании-разработчика позволяют пользователям находить продукт и узнавать о нем. Не следует добавлять в эти метаданные смайлики, эмодзи или повторяющиеся специальные символы. Не используйте при написании только заглавные буквы, если это не часть названия вашего бренда. Не добавляйте в значок приложения символы, вводящие в заблуждение, например индикатор нового сообщения (при отсутствии таких сообщений) или символы скачивания/установки, если приложение не связано со скачиванием контента. В названии приложения должно быть не более 30 символов. В название и значок приложения, а также в имя разработчика нельзя добавлять текст или изображения со сведениями о рейтинге или об успехе приложения в Google Play, ценами и рекламой, а также с информацией об участии в существующих программах Google Play.

Кроме того, в соответствии с правилами Google Play для разработчиков мы можем запросить у вас и другие данные.

Вот примеры наиболее распространенных нарушений:



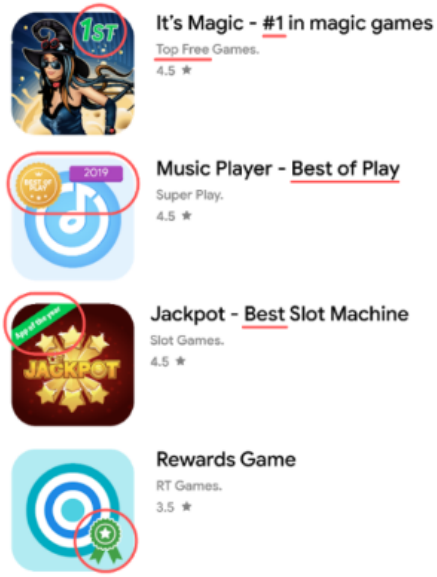
① Анонимные отзывы пользователей.
② Сравнение приложений или брендов.
③ Блоки слов, а также вертикальные или горизонтальные списки слов.



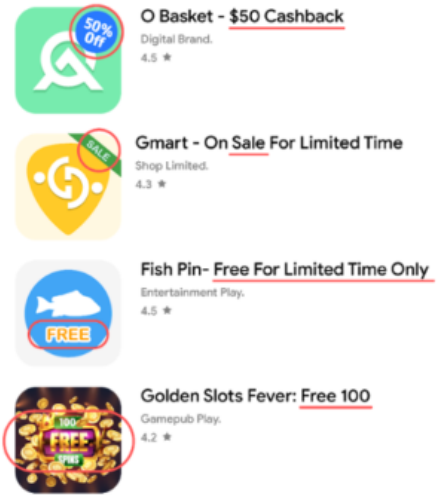
① Слова, состоящие только из заглавных букв (не часть названия бренда).
② Последовательности специальных символов, не имеющие отношения к приложению.

③ Эмодзи, смайлики (включая каомодзи) и специальные символы.
④ Символы, вводящие в заблуждение.
⑤ Текст, вводящий в заблуждение.

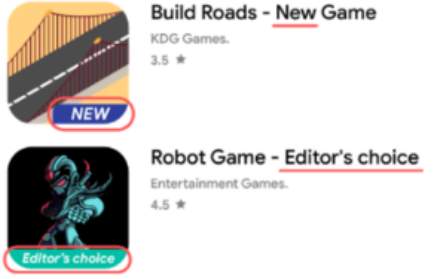
- Изображения или текст с указанием рейтинга или показателей приложения, например значки наград или фразы "Приложение года", "№ 1", "Лучшее приложение Google Play 20XX г.", "Популярное" и т. д.



- Изображения или текст с указанием цены или с рекламной информацией, например "Скидка 10 %", "Кешбэк 500 рублей", "Бесплатно в течение ограниченного времени" и т. д.



- Изображения или текст с указанием программ Google Play, например "Выбор редакции", "Новое" и других.



Вот примеры недопустимого текста, изображений и видео на странице приложения:

- Изображения и видео сексуального характера. Не используйте изображения груди, ягодиц, гениталий и прочие откровенные рисунки и фотографии человеческого тела.
- Непристойная лексика и другие речевые конструкции, недопустимые для широкой аудитории, в описании приложения в Google Play.
- Сцены насилия на значках приложения, в рекламных изображениях и видео.
- Изображение употребления наркотиков, в том числе в образовательном, документальном, научном или художественном контенте. Данные на странице приложения должны подходить для любой аудитории.

Вот несколько советов:

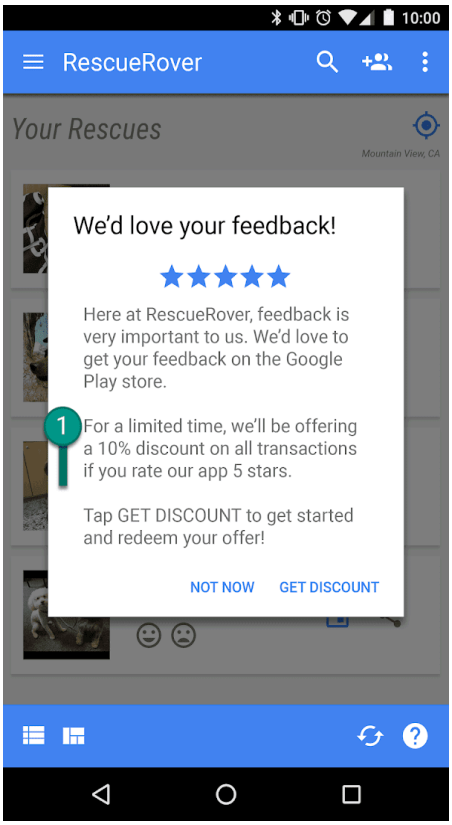
- Расскажите, почему ваше приложение особенное, что выделяет его среди остальных и чем оно может понравиться пользователям.
- Убедитесь, что название и описание дают точное представление о приложении и его функциях.
- Не используйте повторяющиеся или не связанные с приложением ключевые слова и ссылки.
- Описание приложения должно быть простым и понятным. Короткие описания легче читать, особенно на устройствах с небольшим экраном. Слишком длинный, неправильно отформатированный текст, а также лишние подробности и повторы могут нарушать правила Google Play.
- Не забывайте, что страница вашего приложения должна подходить для широкой аудитории. Не используйте в Google Play запрещенные изображения, видео или текст.

Оценки, отзывы и количество установок

Разработчикам запрещено предпринимать попытки искусственно изменить позицию какого-либо приложения в рейтинге Google Play, например с помощью мошеннических установок, оплаченных или ложных оценок и отзывов. Также в приложении не разрешено вознаграждать пользователей за установку других приложений (если это является основным назначением приложения).

Вот примеры наиболее распространенных нарушений:

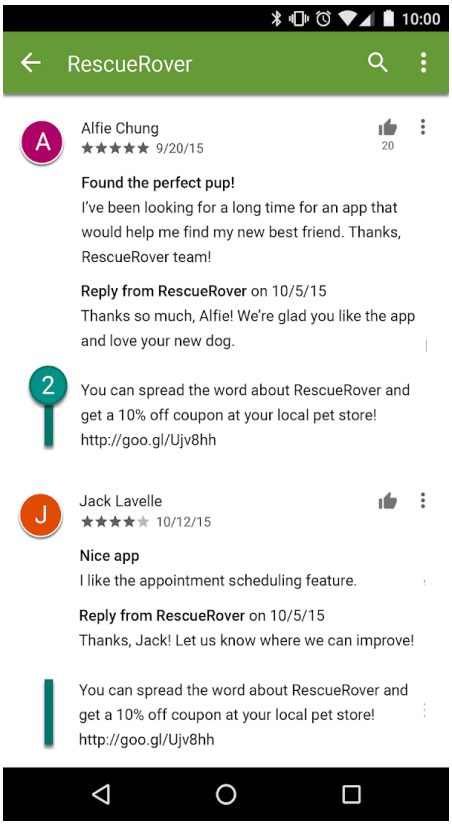
- Просьбы оценить приложение в обмен на поощрение:



① В уведомлении пользователю предлагается скидка в обмен на высокую оценку.

- Попытки изменить позицию приложения в рейтинге Google Play с помощью фальшивых оценок, выставляемых от лица пользователей.

- Публикация отзывов, которые содержат недопустимый контент, и побуждение к этому пользователей. К такому контенту относятся, помимо прочего, информация о партнерах, купонах и игровых кодах, адреса электронной почты и ссылки на веб-сайты или другие приложения.



② В этом отзыве за рекламу приложения пользователям предлагается купон со скидкой.

По оценкам и отзывам можно понять качество приложения. Поэтому они должны быть честными и отражать мнения настоящих пользователей по теме. Вот несколько советов о том, как отвечать на отзывы пользователей.

- Не уклоняйтесь от обсуждения упомянутых проблем и не просите повысить оценку.
- Указывайте справочные ресурсы, например предоставьте адрес электронной почты службы поддержки или URL страницы с часто задаваемыми вопросами.

Возрастные ограничения

Возрастные ограничения в Google Play присваиваются Международной коалицией возрастной классификации (IARC) . Они созданы, чтобы разработчики могли сообщать пользователям, для какой аудитории подходят приложения в их регионе. Устанавливая возрастную категорию контента, представительства IARC в отдельных странах следуют определенным правилам. В Google Play нельзя публиковать приложения без указания возрастных ограничений. Обратите внимание, что реклама в приложениях должна подходить для той же возрастной группы, что и контент приложения, и не быть рассчитана на значительно более взрослую аудиторию. Чтобы узнать дополнительную информацию, прочитайте правила в отношении неприемлемой рекламы .

Для чего нужны возрастные ограничения

Возрастные ограничения помогают клиентам (особенно родителям) понять, есть ли в приложении потенциально нежелательный для них контент. Они позволяют блокировать или фильтровать контент для отдельных пользователей, а также определенных стран и регионов в соответствии с законодательством. С помощью возрастных ограничений можно оценить, есть ли у приложения право участвовать в специальных программах для разработчиков.

Как присваиваются возрастные ограничения

Чтобы определить возрастную категорию, необходимо заполнить анкету в Play Console . В ней нужно подробно описать весь контент в приложении. На основе ваших ответов несколько уполномоченных организаций присвоят приложению определенное возрастное ограничение. Искажение фактов о контенте может привести к удалению или блокировке приложения, поэтому в анкете важно предоставить точную информацию.

Заполнить анкету нужно для каждого приложения независимо от того, опубликовано ли оно в Google Play или только добавлено в Play Console, иначе ему будет присвоен статус "Без классификации". Такие приложения удаляются из Google Play.

Если вы измените контент или функции приложения и это повлияет на ответы в анкете, вам понадобится заполнить ее в Play Console ещё раз.

Возрастное ограничение, которое присваивается после заполнения этой анкеты, относится только к контенту вашего приложения и не затрагивает другие функции и практики, такие как реклама и соглашения с пользователями. Вы обязаны сообщать пользователям обо всех дополнительных возрастных ограничениях, например установленных в связи с мерами по обеспечению конфиденциальности.

Подробную информацию, в том числе об организациях по оценке контента в разных регионах, и инструкции по заполнению анкеты вы найдете в Справочном центре .

Как оспорить возрастное ограничение

Если вы не согласны с присвоенным ограничением, подайте апелляцию напрямую в IARC. Для этого перейдите по ссылке в сертификате, полученном по электронной почте.

Новости и журналы

Для всех новостных приложений и журналов необходимо выбрать категорию "Новости и журналы" в Google Play Console и заполнить декларацию.

В эту категорию включаются все приложения, для которых верно любое из утверждений:

- В Google Play Console разработчик указал, что приложение относится к категории "Новости и журналы".
- В Google Play приложение опубликовано в категории "Новости и журналы", а его название, значок, описание или название компании-разработчика содержит слово "новости" или "журнал".

Узнать больше о том, что считается новостным приложением или журналом, можно из требований к новостным приложениям.

Кроме того, приложения из категории "Новости и журналы" должны:

- приводить источники всех новостных и журнальных статей, включая, помимо прочего, информацию об оригинальных издателях или авторах;
- регулярно пополняться новыми материалами (в приложении не должно быть статического контента);
- предоставлять быстрый и удобный доступ к действительной контактной информации о приложении;
- ясно указывать источники стороннего контента (например, агрегаторы новостей и журналов);
- давать возможность ознакомиться с контентом перед покупкой, если он предоставляется по подписке;
- иметь основную цель, которая не сводится к получению дохода от рекламы или партнерскому маркетингу.

Спам, функциональность и удобство для пользователей

Приложения должны содержать минимальный набор функций и контента и быть интересными для пользователей. Если в приложении постоянно происходят сбои, а также если оно бесполезно или создано для распространения спама среди пользователей либо в Google Play, то публиковать такое приложение не имеет смысла.

Спам

Запрещено публиковать скопированные и низкокачественные приложения, а также приложения, распространяющие спам.

Спам в сообщениях

Запрещено публиковать приложения, которые отправляют от имени пользователя SMS, письма и другие виды сообщений, не давая пользователю возможности проверить содержание и получателя.

Вот пример распространенного нарушения:

- После нажатия кнопки "Поделиться" приложение автоматически отправляет сообщения от имени пользователя. У пользователя нет возможности проверить текст сообщений и выбрать получателей.

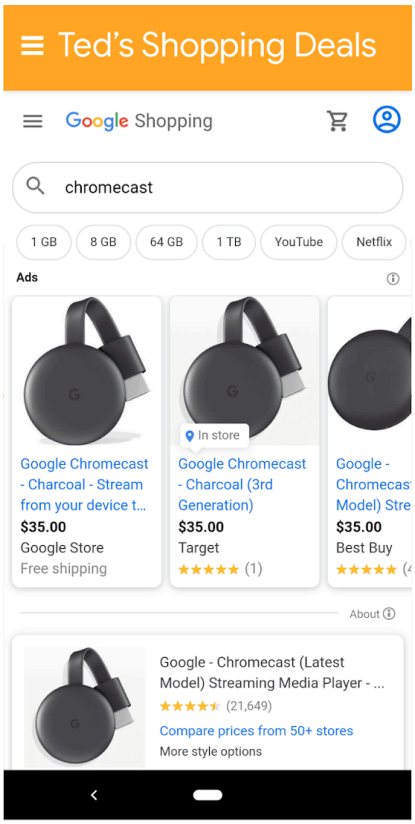
Спам с целью перенаправления трафика

Запрещено публиковать приложения, основной целью которых является привлечение трафика на веб-сайт без разрешения владельца или администратора сайта.

Вот примеры наиболее распространенных нарушений:

- Приложения, основной целью которых является привлечение трафика переходов на веб-сайт для дальнейшего получения бонусов за количество регистраций или покупок на этом веб-сайте.

- Приложения, основной целью которых является привлечение трафика на веб-сайт без разрешения:



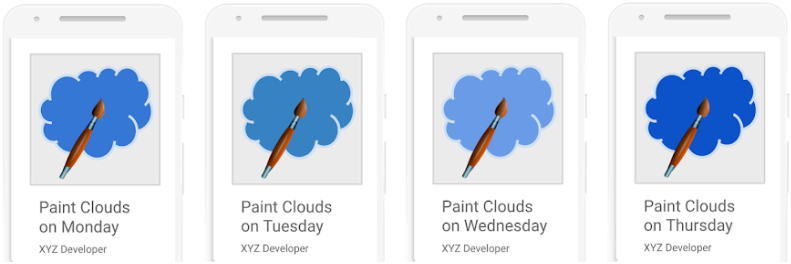
① Это приложение называется "Выгодные товары у Теда" и просто перенаправляет пользователей в Google Покупки.

Повторяющийся контент

Запрещено публиковать приложения, которые полностью повторяют другие приложения, уже размещенные в Google Play. Каждое приложение должно предоставлять уникальный контент или услугу.

Вот примеры наиболее распространенных нарушений:

- Копирование контента из других приложений без переработки и дополнений.
- Создание нескольких приложений с очень похожими функциями, контентом и возможностями. Если объем контента в каждом из таких приложений невелик, возможно, следует опубликовать одно приложение, объединяющее весь контент.



Функциональность, контент и возможности для пользователей

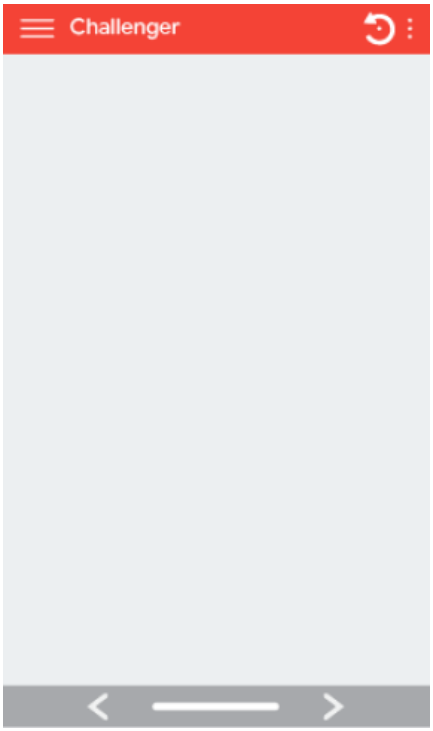
Приложения должны работать стабильно, быть адаптивными и удобными для пользователей, а также предлагать интересные возможности. В Google Play запрещено публиковать бесполезные мобильные приложения, приложения, которые не содержат интересного контента, не имеют ценности для пользователей или в которых постоянно происходят сбои.

Недостаточно функций и контента

Запрещено публиковать приложения, в которых недостаточно функций и контента.

Вот пример распространенного нарушения:

- Приложения, в которых ничего не происходит, если пользователь не задействует встроенные функции (например, сервисы для работы с текстовыми или PDF-файлами).
- Приложения, в которых очень мало контента и нет интересных для пользователя возможностей (например, есть только одни обои).
- Приложения, не выполняющие никаких функций.



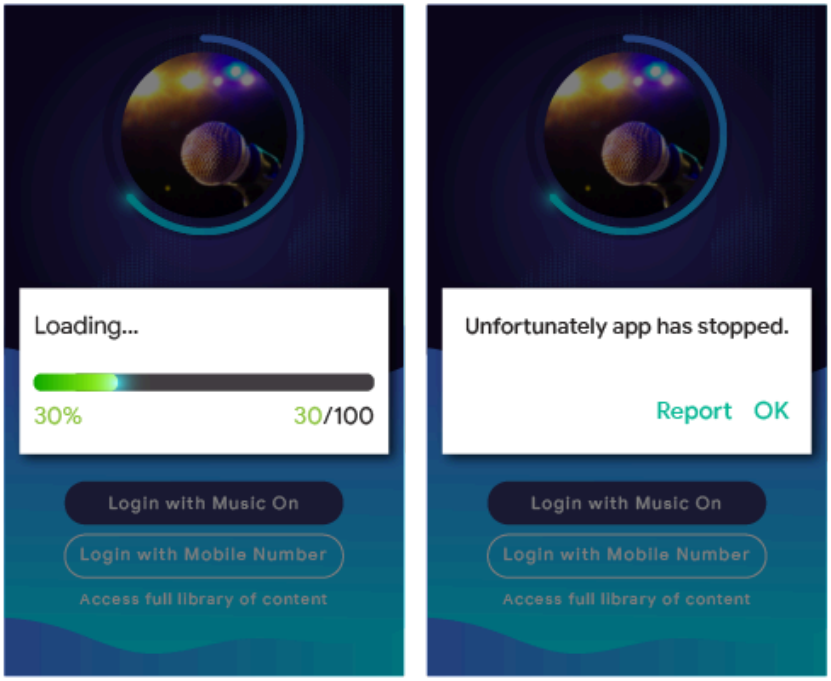
Неработающие приложения

Запрещается публиковать приложения, которые дают сбои, принудительно закрываются, зависают или работают с другими ошибками.

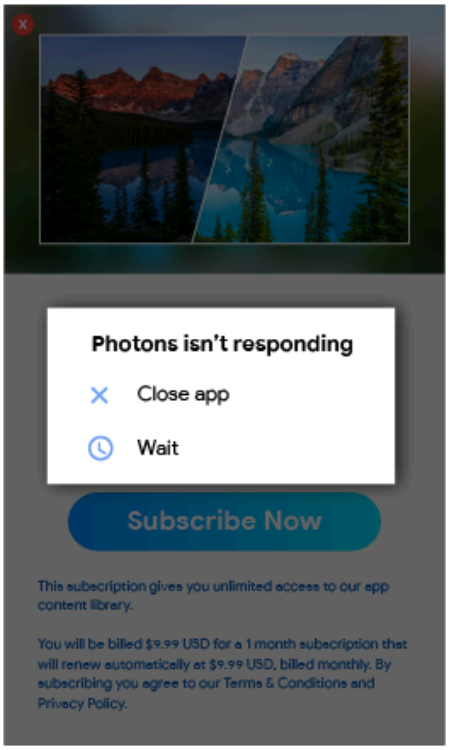
Вот примеры наиболее распространенных нарушений:

- Приложение **не устанавливается**.

- Приложение устанавливается, но **не открывается**.



- Приложения, которые **загружаются, но не отвечают**.



Другие программы

Все приложения, распространяемые через Google Play, должны соответствовать требованиям в отношении контента, которые размещены в этом Центре правил для разработчиков. Однако если приложение создано для особенных функций Android, могут существовать дополнительные

условия. Ознакомьтесь со списком ниже. Возможно, какие-то из этих правил относятся к вашему приложению.

Приложения для Android с мгновенным запуском

Приложения для Android с мгновенным запуском должны быть удобными в использовании, а также соответствовать стандартам конфиденциальности и безопасности. Чтобы добиться этого, мы разработали специальные правила.

Разработчики, желающие распространять через Google Play приложения для Android с мгновенным запуском, должны соблюдать эти правила наряду с остальными Правилами программы для разработчиков.

Идентификация

Если приложение с мгновенным запуском предполагает вход в аккаунт, в него необходимо интегрировать функцию Smart Lock для паролей .

Поддержка ссылок

Если необходимо перенаправить пользователя из одного приложения в другое, следует реализовать переход в приложение с мгновенным запуском (если это возможно), а не использовать компонент WebView .

Технические характеристики

При разработке приложений с мгновенным запуском обязательно соблюдайте технические требования Google, которые могут меняться время от времени, в том числе требования, перечисленные в открытой документации .

Предложение установить приложение

Приложение с мгновенным запуском может предлагать установить приложение, но это не должно быть его основной функцией. Кроме того, должны соблюдаться следующие требования:

- Используется стандартный значок Material Design "Установить" и кнопка с надписью "Установить".
- Используется не более 2–3 скрытых предложений установить приложение.
- Предложение об установке не похоже на рекламу (например, нельзя использовать баннеры).

Дополнительные сведения и указания можно найти в этой статье .

Внесение изменений в устройство

Приложение с мгновенным запуском не должно вносить в устройство пользователя изменения, которые сохраняются дольше, чем работает само приложение. Например, оно не должно менять обои или создавать виджет на главном экране.

Видимость работы приложения

Пользователь должен знать, что приложение с мгновенным запуском работает. Скрывать факт работы приложения от пользователя нельзя.

Идентификаторы устройства

У приложения с мгновенным запуском не должно быть доступа к идентификаторам устройства, которые остаются после завершения работы приложения, если при этом пользователь не может сменить их. Несколько примеров:

- Номер Build Serial;
- MAC-адреса любых сетевых процессоров;
- IMEI-код и номер IMSI.

Приложение может получить доступ к номеру телефона с разрешения пользователя. Разработчик не должен пытаться определить личность пользователя с помощью этих идентификаторов или других данных.

Сетевой трафик

Сетевой трафик внутри приложения с мгновенным запуском должен шифроваться с помощью протокола стандарта TLS, например HTTPS.

Правила Android в отношении эмодзи

Правила в отношении эмодзи призваны обеспечить инклюзивное и единообразное взаимодействие между пользователями. В связи с этим все приложения для Android 12 и выше должны поддерживать последнюю версию эмодзи Unicode .

Они уже доступны в приложениях, использующих эмодзи по умолчанию, без пользовательской реализации, на Android 12 и выше.

Приложения с пользовательскими эмодзи, в том числе из сторонних библиотек, должны полностью поддерживать последнюю версию Unicode при работе на Android 12 и выше в течение 4 месяцев после выпуска новых эмодзи Unicode.

Инструкции по поддержке современных эмодзи содержатся в руководстве .

Семьи

Google Play – это удобная платформа, где разработчики могут публиковать приложения для пользователей любых возрастов. Прежде чем включать приложение в программу "Приложения для всей семьи" или добавлять в Google Play приложение, целевой аудиторией которого являются дети, убедитесь, что оно действительно подходит для детей и соответствует законодательству.

В Академии для разработчиков можно узнать о требованиях к приложениям для детей и проверке по интерактивному контрольному списку.

Правила программы Google Play "Приложения для всей семьи"

Когда родители выбирают контент для своих детей, они хотят, чтобы он был качественным и безопасным. На этой странице рассказано, каким требованиям должны соответствовать приложения, которые предназначены для всей семьи или только для детей.

Понятие "дети" может трактоваться по-разному в зависимости от страны и ситуации. Чтобы узнать, какие возрастные ограничения применяются к вашему приложению и какие обязательства вы должны соблюдать как его разработчик, проконсультируйтесь с юристом. Вы знаете свое приложение лучше всех, и только от вас зависит, будет ли оно безопасным для детей.

Разработчики могут запросить оценку приложений, соответствующих правилам программы Google Play "Приложения для всей семьи", для участия в программе "Одобрено преподавателями", но мы не гарантируем, что они будут в нее включены.

Требования к приложению в Play Console

Целевая аудитория и контент

Перед публикацией приложения необходимо выбрать возрастную группу в разделе Целевая аудитория и контент в Google Play Console. Независимо от того, какую группу вы укажете, мы будем учитывать, есть ли в вашем приложении изображения и фразы, из-за которых приложение можно счесть ориентированным на детей. Команда Google Play оставляет за собой право проверять предоставленную информацию о приложении и определять, точно ли выбрана целевая аудитория.

Несколько возрастных групп можно выбрать только в том случае, если вы точно уверены, что приложение подходит для всех них. Например, контент для малышей и дошкольников должен относиться только к категории "До 5 лет". Если вы разработали приложение для учеников определенного класса, выберите наиболее подходящий возраст. Группы, включающие и взрослых, и детей, можно указывать, только если ваше приложение действительно предназначено для всех возрастов.

Обновления раздела "Целевая аудитория и контент"

Вы можете в любой момент изменить информацию в разделе "Целевая аудитория и контент" в Google Play Console. Чтобы новые сведения появились в Google Play, необходимо выпустить обновление, однако проверить их мы можем ещё до того, как вы загрузите новую версию приложения.

Если вы изменили целевую аудиторию, добавили в приложение рекламу или платный контент, мы настоятельно рекомендуем сообщить об этом пользователям. Для этого можно использовать раздел "Что нового" на странице в Google Play или уведомления в самом приложении.

Искажение фактов в Play Console

Искажение фактов о приложении в Play Console, в том числе в разделе "Целевая аудитория и контент", может привести к удалению или блокировке приложения, поэтому важно предоставить как можно более точную информацию.

Требования к приложениям для детей

Если в вашу целевую аудиторию входят дети, вы должны выполнять перечисленные ниже требования. Их несоблюдение может привести к удалению или блокировке приложения.

1. **Контент приложения.** Детям должен быть доступен только подходящий для них контент. Если в приложении есть контент, допустимый не везде, оно может быть доступно только в регионе, где такой контент считается подходящим для детей (ограничения по регионам).
2. **Функции приложения.** Основной целью приложения не должна быть демонстрация сайта через компонент WebView или привлечение трафика на сайт без разрешения его владельца или администратора.
3. **Ответы на вопросы в Play Console.** В Play Console необходимо точно отвечать на вопросы о приложении, а также обновлять предоставленную информацию, если в нем что-то меняется. Помимо прочего, требуется указывать достоверные данные в разделе "Целевая аудитория и контент", разделе безопасности данных и анкете IARC для присвоения возрастного ограничения.
4. **Работа с данными.** Если ваше приложение собирает какую-либо личную и конфиденциальную информацию детей, в том числе с помощью API и SDK, вы обязаны сообщить об этом в явной форме. К конфиденциальной информации детей относятся, например, учетные данные, данные с микрофона и камеры, сведения на устройстве, идентификатор Android и данные об использовании объявлений. Также убедитесь, что приложение соответствует следующим требованиям:
   - Приложения, предназначенные только для детей, не должны передавать рекламный идентификатор Android (AAID), серийный номер SIM-карты, серийный номер сборки, BSSID, MAC-адрес, SSID, IMEI-код и/или номер IMSI.
     - Приложения, единственной целевой аудиторией которых являются дети, не должны запрашивать разрешение AD_ID при использовании Android API уровня 33 и выше.

- Приложения, предназначенные для детей и взрослых, не должны передавать рекламный идентификатор AAID, серийный номер SIM-карты, серийный номер сборки, BSSID, MAC-адрес, SSID, IMEI-код и/или номер IMSI, если пользователь ребенок или его возраст неизвестен.
- Нельзя запрашивать номер телефона при помощи класса TelephonyManager в Android API.
- Приложения, предназначенные только для детей, не должны запрашивать доступ к данным о местоположении, а также собирать, использовать и передавать информацию о точном местоположении.
- Для запроса подключения по Bluetooth необходимо использовать CompanionDeviceManager . Исключение – приложения, предназначенные только для версий ОС, которые не поддерживают этот класс.

5. **API и SDK.** Убедитесь, что API и SDK используются в вашем приложении надлежащим образом.
   - Приложения, предназначенные только для детей, не должны использовать API или SDK, которые не одобрены для сервисов, рассчитанных в основном на такую целевую аудиторию.
     - Это относится в том числе к API, использующим для аутентификации и авторизации технологию OAuth, в условиях использования которых сказано, что они не одобрены для сервисов, предназначенных для детей.
   - В приложениях, предназначенных для детей и взрослых, нельзя использовать API или SDK, которые не одобрены для сервисов, рассчитанных на детей. Исключения возможны, если API или SDK применяются только после нейтрального возрастного фильтра или если при их использовании данные детей не собираются. Кроме того, такие приложения не должны требовать, чтобы пользователи получали доступ к контенту через API или SDK, не одобренные для сервисов, которые предназначены для детей.

6. **Дополненная реальность.** Если в приложении используется дополненная реальность, при запуске разделов с ней должно появляться предупреждение, содержащее следующую информацию:
   - Напоминание о важности родительского контроля.
   - Напоминание об опасности объектов реального мира (например, "Обращайте внимание на предметы и людей вокруг").
   - Для использования приложения не должны требовать устройства, не рекомендованные для детей (например, Daydream или Oculus).

7. **Социальные приложения и функции.** Если ваше приложение позволяет пользователям делиться или обмениваться информацией, вы должны в точности описать эти функции в анкете для присвоения возрастного ограничения в Play Console.
   - Социальные приложения. Их основная цель – предоставлять возможность делиться контентом в свободной форме или общаться с большими группами людей. Во всех социальных приложениях, в целевую аудиторию которых входят дети, перед предоставлением пользователям доступа к обмену контентом или информацией должны показываться напоминания о том, как защитить себя в интернете и к каким рискам в реальном мире может привести онлайн-взаимодействие. Кроме того, прежде чем позволять детям обмениваться личной информацией, вы должны требовать действия со стороны взрослого.
   - Социальные функции. Это любые дополнительные функции приложения, позволяющие делиться контентом в свободной форме или общаться с большими группами людей. Если в приложении есть социальные функции и в его целевую аудиторию входят дети, перед предоставлением пользователям доступа к обмену контентом и информацией вы должны показывать напоминания о том, как защитить себя в интернете и к каким рискам в реальном мире может привести онлайн-взаимодействие. Кроме того, взрослым необходимо предоставить возможность управлять настройками социальных функций, в том числе включать и отключать их или выбирать различные уровни функциональности для детей. Наконец, прежде чем включать функции, которые позволяют детям обмениваться личной информацией, вы должны требовать действия со стороны взрослого.

- Для этого у вас должен быть механизм, позволяющий убедиться, что пользователь не является ребенком, и не побуждающий детей неверно указывать свой возраст, чтобы получать доступ к разделам, предназначенным для взрослых (например, вы можете запрашивать PIN-код взрослого, пароль, дату рождения, подтверждение адреса электронной почты, удостоверение личности с фотографией, данные кредитной карты или номер социального страхования).
- Дети не должны входить в целевую аудиторию социальных приложений, основная цель которых – общение с незнакомыми людьми. Это могут быть чат-рулетки, приложения для свиданий, детские открытые чат-комнаты и т. д.

8. **Соблюдение законодательства.** Ваше приложение и все вызываемые или используемые им API и SDK не должны нарушать закон США О защите личных сведений детей в интернете (COPPA), Генеральный регламент ЕС о защите персональных данных (GDPR), а также другие действующие законы и правила.

Вот примеры наиболее распространенных нарушений:

- Приложения, которые рекламируются как игры для детей, но на самом деле подходят только для взрослых.
- Приложения, применяющие те API, которые по своим условиям использования запрещены для ориентированных на детей сервисов.
- Приложения, в которых употребление табака, алкоголя или запрещенных веществ упоминается в привлекательной форме.
- Азартные игры и имитирующие их приложения.
- Приложения, содержащие сцены насилия и кровопролития, а также другой шокирующий контент, не подходящий для детей.
- Приложения, предназначенные для знакомств или содержащие рекомендации брачного или сексуального характера.
- Приложения, содержащие ссылки на сайты, контент которых нарушает Правила программы для разработчиков .
- Приложения, в которых детям показывают рекламу для взрослых (например, связанную с насилием, азартными играми, контентом сексуального характера).

Реклама и монетизация

Если вы монетизируете в Google Play приложение, предназначенное для детей, оно должно соответствовать приведенным ниже требованиям в отношении рекламы и монетизации.

Эти требования относятся к любой монетизации и рекламе ваших и сторонних приложений, перекрестному продвижению, покупкам в приложении и другому коммерческому контенту (например, к продакт-плейсменту). Ничто из перечисленного также не должно нарушать действующие законы и нормы, в том числе корпоративные и отраслевые.

Команда Google Play оставляет за собой право отклонять, удалять и блокировать приложения, в которых слишком настойчиво предлагается платный контент.

Требования к рекламе

Если в приложении появляется реклама для детей или пользователей, чей возраст неизвестен, необходимо:

- использовать для показа рекламы этим лицам только рекламные SDK, прошедшие самостоятельную сертификацию в рамках Программы рекламы в приложениях для всей семьи;
- исключить для таких пользователей ремаркетинг (рекламу, направленную на отдельных пользователей и зависящую от истории взаимодействия с сайтом или приложением) и рекламу на основе интересов (рекламу, направленную на отдельных пользователей, чье поведение в интернете соответствует определенным характеристикам);

- убедиться, что контент в рекламе для таких пользователей можно показывать детям;
- убедиться, что реклама для таких пользователей соответствует требованиям к формату объявлений для всей семьи;
- обеспечить соблюдение действующего законодательства и отраслевых стандартов, касающихся рекламы для детей.

Требования к форматам объявлений

Реклама и средства монетизации в вашем приложении не должны содержать вводящий в заблуждение контент или быть оформленными таким образом, что это может привести к случайным кликам со стороны несовершеннолетних пользователей.

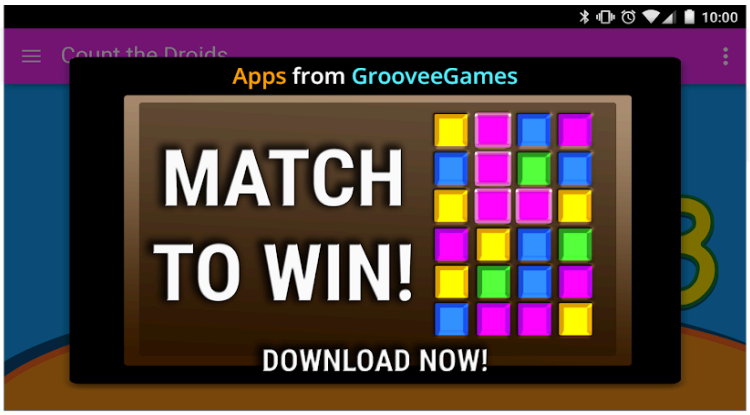
Ниже перечислены приемы, которые запрещено использовать в приложениях, единственной целевой аудиторией которых являются дети, а также при показе рекламы детям или лицам неизвестного возраста в приложениях, целевой аудиторией которых являются дети и лица старшего возраста.

- Реклама и средства монетизации, которые прерывают работу приложения, в том числе занимают весь экран, не позволяют нормально использовать приложение и не закрываются явным способом (например, полноэкранные объявления, которые сложно закрыть).
- Реклама и средства монетизации, которые мешают нормальному использованию приложения или игры (в том числе объявления с вознаграждением и разрешенные пользователем объявления) и которые нельзя закрыть через пять секунд.
- Реклама и средства монетизации, которые не мешают нормальной работе приложения или игры, могут не закрываться через пять секунд (например, видеоклип со встроенной рекламой).
- Межстраничная реклама и средства монетизации, которые появляются сразу после запуска приложения.
- Размещение нескольких объявлений на странице. Например, одновременный показ более одного баннера или видеообъявления и рекламные баннеры, которые содержат несколько предложений в одном месте размещения.
- Реклама и средства монетизации, которые сложно отличить от контента приложения. Например, окна Offerwall и другие объявления с эффектом присутствия.
- Использование шокового эффекта или тактик эмоционального манипулирования, чтобы провоцировать пользователей на просмотр объявлений или покупку в приложении.
- Вводящие в заблуждение объявления, которые заставляют пользователя переходить по ссылкам с помощью кнопки "Закрыть", открывающей другое объявление, или внезапного появления в тех частях экрана, на которые пользователь обычно нажимает для доступа к другим функциям приложения.
- Отсутствие четкого указания на различия между виртуальной валютой и реальными деньгами при покупках в приложении.

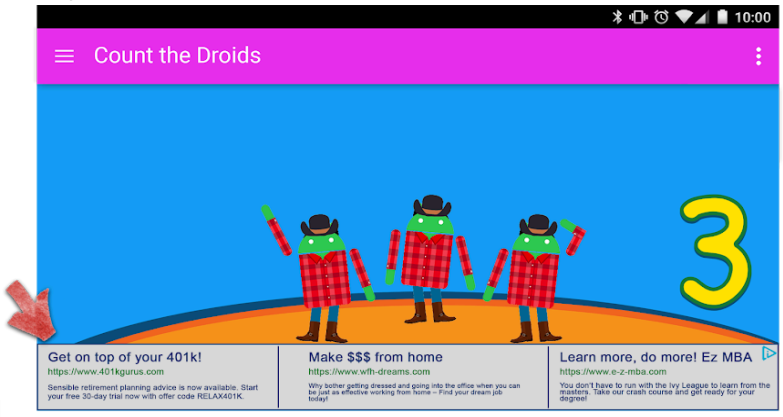
Вот примеры наиболее распространенных нарушений:

- Реклама и элементы монетизации, которые перемещаются по экрану, чтобы их нельзя было закрыть.
- Реклама и элементы монетизации, которые нельзя закрыть через пять секунд с момента их появления:

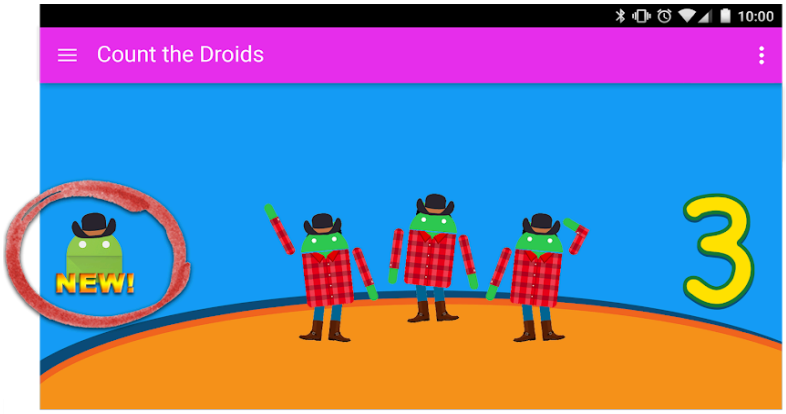
- Реклама и элементы монетизации, которые занимают большую часть экрана и которые трудно закрыть из-за отсутствия специальных кнопок.



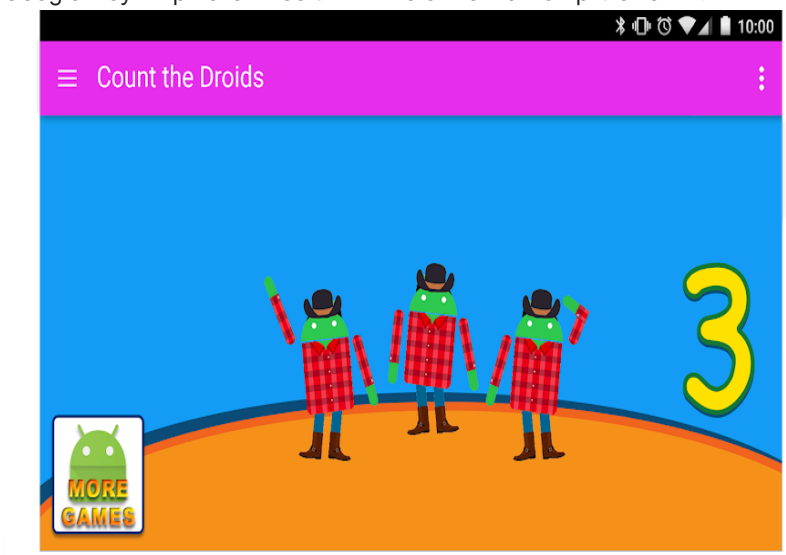
- Баннеры с несколькими объявлениями.



- Реклама и элементы монетизации, которые можно принять за контент приложения.



- Кнопки, объявления или иные элементы монетизации, рекламирующие другие продукты в Google Play и при этом неотличимые от контента приложения.



Примеры объявлений, которые нельзя показывать детям:

- **Недопустимый мультимедийный контент.** Реклама сериалов, фильмов и музыкальных альбомов, не предназначенных для детей.
- **Недопустимые видеоигры и скачиваемое ПО.** Реклама видеоигр и программ, не предназначенных для детей.
- **Запрещенные или вредные вещества.** Реклама алкоголя, табака, наркотических и психотропных веществ, а также любых других веществ, которые могут приносить вред здоровью.
- **Азартные игры.** Реклама азартных игр, тотализаторов, а также любых других денежных соревнований или конкурсов, в том числе тех, где пользователям не нужно платить, чтобы принять участие.
- **Контент для взрослых и материалы сексуального характера.** Реклама с эротическим, непристойным содержанием и материалами для взрослых.
- **Знакомства и отношения.** Реклама сайтов знакомств.
- **Насилие.** Реклама, содержащая откровенные сцены насилия или другие изображения, неподходящие для детей.

Рекламные SDK

При размещении рекламы в приложении, предназначенном только для детей, необходимо использовать исключительно версии рекламных SDK, прошедшие самостоятельную

сертификацию в рамках нашей программы . Если приложение рассчитано как на детей, так и на взрослых, вы должны предусмотреть проверку возраста пользователя (например, с помощью нейтрального возрастного фильтра) и убедиться, что дети будут видеть только те объявления, для которых использовались версии рекламных SDK, прошедшие самостоятельную сертификацию в рамках программы Google Play.

Подробную информацию об этих требованиях вы найдете на странице с правилами Программы самостоятельной сертификации рекламных SDK в приложениях для всей семьи . Посмотреть текущий список версий рекламных SDK, которые прошли самостоятельную сертификацию, можно здесь .

Если вы используете сервис AdMob, уточните информацию по работе с ним в Справочном центре .

Вы должны самостоятельно проверять, соответствует ли ваше приложение требованиям к рекламе, покупкам в приложении и коммерческому контенту. Уточните действующие правила у своих поставщиков рекламных SDK.

Правила Программы самостоятельной сертификации рекламных SDK в приложениях для всей семьи

Мы хотим сделать использование платформы Google Play безопасным для детей и всей семьи. В частности, мы стремимся защищать личные данные несовершеннолетних и показывать им только те объявления, которые предназначены для их возрастной группы. Мы требуем от разработчиков платформ медиации и рекламных SDK самостоятельно подтверждать, что их решения подходят для детей и соответствуют Правилам программы для разработчиков приложений в Google Play и правилам программы "Приложения для всей семьи" , в том числе требованиям Программы самостоятельной сертификации рекламных SDK в приложениях для всей семьи .

Эта программа помогает разработчикам определять, какие рекламные SDK и платформы медиации прошли самостоятельную сертификацию и могут использоваться в приложениях, разработанных специально для детей.

Искажение фактов о своем SDK, в том числе в заявке на участие , может привести к удалению SDK из Программы самостоятельной сертификации рекламных SDK в приложениях для всей семьи или его блокировке, поэтому убедитесь, что вы предоставляете точную информацию.

Требования

SDK и платформы медиации, обслуживающие приложения, которые участвуют в программе "Для всей семьи", должны отвечать правилам для разработчиков Google Play, в том числе приведенным ниже. Несоответствие любому из требований может привести к удалению SDK или платформы медиации из Программы самостоятельной сертификации рекламных SDK в приложениях для всей семьи или блокировке доступа к этой программе.

Вы несете ответственность за то, чтобы в ваших SDK и на платформах медиации выполнялись указанные требования. Ознакомьтесь с Правилами программы для разработчиков приложений в Google Play, правилами программы "Приложения для всей семьи" и требованиями Программы самостоятельной сертификации рекламных SDK в приложениях для всей семьи.

1. **Содержание объявления.** Если ваши объявления доступны детям, их содержание должно соответствовать возрастным ограничениям.
   - Вам необходимо: 1) дать определение нежелательным объявлениям и поведению; 2) запретить их в условиях использования или правилах SDK или платформы. Определения должны соответствовать Правилам программы для разработчиков приложений в Google Play.
   - Обязательно выберите способ, с помощью которого вы будете присваивать объявлениям возрастные ограничения. Необходимо настроить не менее двух категорий: "Для всех" и "Для

взрослых". Возрастные ограничения должны присваиваться по той же системе, которую Google предоставляет поставщикам SDK после заполнения специальной формы .

- Если для показа рекламы детям используется назначение ставок в реальном времени, обязательно убедитесь, что креативы проверены и соответствуют всем требованиям выше.
- У вас также должен быть способ визуальной идентификации креативов, который обозначает их принадлежность к вашему инвентарю, например водяной знак с логотипом вашей компании.

2. **Формат объявления.** Необходимо, чтобы все объявления, которые видны детям, соответствовали требованиям к формату объявлений для всей семьи. Вы должны обеспечить разработчикам возможность выбирать форматы, отвечающие правилам программы Google Play "Приложения для всей семьи".
   - Реклама не должна содержать вводящий в заблуждение контент или элементы, которые могут привести к случайным кликам со стороны несовершеннолетних пользователей. Сюда относятся объявления, которые заставляют пользователей переходить по ссылкам с помощью кнопки "Закрыть", открывающей другое объявление, или внезапного появления в тех частях экрана, на которые пользователи обычно нажимают для доступа к другим функциям приложения.
   - Недопустима избыточная реклама, в том числе элементы, которые занимают весь экран, не позволяют нормально использовать приложение и не закрываются явным способом, например полноэкранные объявления, которые сложно закрыть.
   - Для объявлений, которые мешают нормальной работе приложения или игры, необходимо добавить возможность закрыть их через 5 секунд.
   - Запрещено размещение нескольких объявлений на странице. Например, одновременный показ более одного баннера или видеообъявления и рекламные баннеры, которые содержат несколько предложений в одном месте размещения.
   - Реклама должна явно отличаться от контента приложения. Окна Offerwall и объявления с эффектом присутствия, которые несовершеннолетний пользователь не посчитает рекламой, запрещены.
   - В объявлениях нельзя использовать шоковый эффект или тактики эмоционального манипулирования, чтобы провоцировать пользователей на просмотр рекламы или покупку в приложении.
3. **Реклама на основе интересов или ремаркетинг.** Обязательно убедитесь, что объявления, которые видны детям, не основаны на их интересах (т. е. не направлены на отдельных пользователей, чье поведение в интернете соответствует определенным характеристикам) и не показываются с использованием ремаркетинга (т. е. не направлены на отдельных пользователей в зависимости от истории взаимодействия с сайтом или приложением).
4. **Работа с данными.** Как поставщик SDK, вы обязаны объяснить пользователям, каким образом будете обрабатывать их данные, например сведения с устройств. Обязательно сообщите, как и для чего SDK будет использовать и собирать данные, а также получать и предоставлять к ним доступ. Применять информацию в целях, о которых вы не заявили, запрещено. Эти правила Google Play дополняют требования действующего законодательства о конфиденциальности и защите данных. Если ваше приложение собирает какую-либо личную и конфиденциальную информацию детей, вы обязаны сообщить об этом в явной форме. К конфиденциальной информации детей, помимо прочего, относятся учетные данные, данные с микрофона и камеры, сведения на устройстве, идентификатор Android и данные об использовании объявлений.
   - Вам необходимо разрешить разработчикам запрашивать показ объявлений, ориентированных на детей (в определенных приложениях или в каждом конкретном случае). Убедитесь, что контент в объявлениях не нарушает действующее законодательство, например закон США "О защите личных сведений детей в интернете" (COPPA) и Генеральный регламент ЕС о защите персональных данных (GDPR) .

- Кроме того, в рекламных SDK, которые используются на ресурсах для детей, нужно отключить персонализированную рекламу, объявления на основе интересов и ремаркетинг.
- Если для показа рекламы детям используется назначение ставок в реальном времени, убедитесь, что участникам аукциона присваиваются индикаторы конфиденциальности.
- Приложения не должны передавать AAID, серийный номер SIM-карты и сборки, BSSID, MAC-адрес, SSID, IMEI-код и номер IMSI, запрошенный у детей и пользователей, чей возраст неизвестен.

5. **Платформы медиации.** При показе рекламы детям:
   - Следует применять только рекламные SDK, прошедшие самостоятельную сертификацию для использования в приложениях для всей семьи, или принимать меры защиты, гарантирующие, что все объявления на платформе медиации будут соответствовать этим требованиям.
   - Необходимо передавать информацию о возрастных ограничениях для рекламного контента и о том, что ресурс предназначен для детей.
6. **Самостоятельная сертификация и соответствие правилам.** Вы должны предоставить Google все необходимые сведения, в частности обозначенные в специальной форме , чтобы подтвердить соответствие рекламного SDK всем требованиям к самостоятельной сертификации. Помимо прочего, вам нужно:
   - Добавить документы на английском языке: условия использования, политику конфиденциальности и руководство по интеграции вашего SDK или платформы медиации.
   - Предоставить тестовый вариант приложения с последней версией рекламного SDK, соответствующей требованиям. Такое приложение должно представлять собой полностью собранный исполняемый APK-файл для Android, использующий все функции указанного SDK. Необходимо, чтобы тестовое приложение:
     - было отправлено нам в виде полностью собранного исполняемого APK-файла для смартфонов с ОС Android;
     - использовало рекламный SDK последней выпущенной или готовящейся к выпуску версии, соответствующий правилам Google Play;
     - задействовало все функции рекламного SDK, в том числе отправку запросов для получения и показа объявлений;
     - по запросу предоставляло полный доступ ко всему рекламному инвентарю, который показывается пользователю;
     - не ограничивало доступ в зависимости от местоположения;
     - позволяло определять возраст пользователей и показывать креативы из инвентаря, подходящего для конкретной возрастной группы (если ваш инвентарь предназначен для пользователей всех возрастов);
     - показывало все объявления из вашего инвентаря (когда нейтральный возрастной фильтр отключен).
7. Вы обязаны своевременно отвечать на любые последующие запросы информации и самостоятельно сертифицировать каждую отправленную версию на соответствие последним Правилам программы для разработчиков приложений в Google Play, включая требования к приложениям для всей семьи.
8. **Юридические требования.** Рекламные SDK, прошедшие самостоятельную сертификацию для использования в приложениях для всей семьи, необходимо применять для показа объявлений в соответствии со всеми законами и положениями относительно детей, касающимися издателей.
   - Ваши SDK и платформы медиации не должны нарушать закон США О защите личных сведений детей в интернете (COPPA), Генеральный регламент ЕС о защите персональных данных (GDPR), а также другие действующие законы и правила.

   Примечание. Понятие "дети" может трактоваться по-разному в зависимости от страны и

ситуации. Чтобы узнать, какие возрастные ограничения применяются к вашему приложению и какие обязательства вы должны соблюдать, проконсультируйтесь с юристом. Именно разработчики, знающие свои продукты лучше всех, помогают нам делать приложения в Google Play безопасными для всей семьи.

Более подробную информацию о требованиях вы найдете на странице с правилами Программы самостоятельной сертификации рекламных SDK в приложениях для всей семьи.

Контроль за соблюдением правил

Лучше избегать нарушений, чем устранять их. Если же проблема уже возникла, мы хотим, чтобы разработчики понимали, как исправить свои приложения и привести их в соответствие с нашими правилами. При обнаружении нарушений или возникновении вопросов о нарушении сообщите нам об этом.

Сфера действия правил

Эти правила распространяются на любые материалы (включая рекламу и пользовательский контент), которые содержит или показывает ваше приложение либо на которые оно ссылается, а также на общедоступную информацию в вашем аккаунте разработчика Google Play (включая ваше имя и целевую страницу сайта).

Запрещено публиковать приложения, которые позволяют устанавливать другие приложения. Если ваши приложения обеспечивают доступ к другим приложениям, играм или ПО без установки, в том числе к функциям, предоставленным третьими лицами, вы должны гарантировать, что весь контент, к которому приложения предоставляют доступ, соответствует правилам Google Play. Такие приложения могут подвергаться дополнительной проверке на соблюдение правил.

В правилах используются те же термины, что и в Соглашении о распространении программных продуктов. Ваше приложение обязано соответствовать требованиям правил и соглашения, а также иметь рейтинг в соответствии с нашей системой возрастных ограничений.

Запрещено публиковать приложения, подрывающие доверие пользователей к экосистеме Google Play. Принимая решение о публикации приложений в Google Play, мы учитываем ряд факторов, в том числе вероятность вредоносного поведения или злоупотребления. Вероятность злоупотребления оценивается на основе различных сведений, включая историю нарушений, жалобы на приложение и разработчика, отзывы пользователей, а также использование популярных брендов, персонажей и других объектов.

Как это работает

Google Play Защита проверяет приложения во время установки, а также периодически сканирует ваше устройство. Если будет обнаружено потенциально опасное приложение, сервис:

- Отправит вам уведомление. Чтобы защитить свое устройство, нажмите на уведомление и выберите "Удалить".
- Заблокирует приложение, если вы его не удалите.
- Удалит приложение. Чаще всего опасные приложения удаляются автоматически, после чего появляется уведомление об этом.

Защита от вредоносного ПО

Чтобы защищать вас от вредоносного стороннего ПО, мошеннических сайтов и других угроз, Google может получать сведения о:

- сетевых подключениях вашего устройства;
- потенциально опасных URL;

- приложениях из Google Play и сторонних источников, установленных на вашем устройстве, а также об операционной системе.

Если приложение или URL покажется нам подозрительным, вы получите предупреждение. Мы оставляем за собой право блокировать и удалять приложения или URL, которые могут нанести вред устройству, данным или пользователю.

Вы можете отключить некоторые функции защиты в настройках устройства, но Google по-прежнему будет получать сведения о приложениях, установленных через Google Play. Приложения из сторонних источников все равно будут проверяться, хотя информация о них не будет отправляться в Google.

Как работают оповещения о нарушениях конфиденциальности

Если мы удалим из Google Play приложение, которое может получить доступ к вашим персональным данным, вы получите уведомление об этом и сможете удалить приложение с устройства.

Контроль за соблюдением правил

Проверяя контент и аккаунты на предмет нарушения законодательства или наших правил, мы принимаем решение на основе различной информации. Помимо прочего, к ней относятся метаданные приложения (например, его название и описание), функции приложения и сторонний код в нем, сведения об аккаунте (например, история нарушения правил), результаты наших прошлых проверок и, если применимо, другая информация, полученная через механизмы для отправки жалоб. Вы обязаны убедиться, что любой сторонний код (например, SDK) в вашем приложении и относящиеся к этому приложению процессы обработки данных на стороне создателя кода соответствуют всем Правилам программы для разработчиков приложений в Google Play.

Если ваше приложение или аккаунт разработчика нарушает какие-либо наши правила, мы примем соответствующие меры, описанные ниже. Мы предоставим вам информацию о своих действиях по электронной почте, а также сообщим, как подать апелляцию, если вы считаете, что произошла ошибка.

Обратите внимание, что при удалении или отправке предупреждения могут указываться не все нарушения, обнаруженные в вашем аккаунте, приложении или каталоге приложений. Разработчики обязаны сами устранить остальные нарушения и проверить свой контент на соответствие нашим правилам. Если вы не устраните нарушения в аккаунте и всех своих приложениях, мы можем принять дополнительные принудительные меры.

Повторные или серьезные нарушения этих правил (например, мошенничество или размещение вредоносного ПО) или нарушение Соглашения о распространении программных продуктов приведет к удалению личного аккаунта или связанных с ним аккаунтов разработчика Google Play.

Принудительные меры

Принудительные меры могут иметь разные последствия для ваших приложений. За проверку приложений и контента в них, выявление и оценку материалов, которые нарушают наши правила и причиняют вред пользователям, а также экосистеме Google Play в целом, в Google отвечают как люди, так и автоматизированные системы. Последние позволяют нам находить больше нарушений и быстрее анализировать потенциальные проблемы, что, в свою очередь, помогает обеспечивать безопасность Google Play. Автоматизированные системы либо удаляют контент, нарушающий правила, либо передают его подготовленным операторам и аналитикам, если требуется более тщательная проверка или понимание контекста. Результаты проверок вручную затем используются для улучшения моделей машинного обучения.

Ниже представлены возможные действия со стороны Google Play и их потенциальные последствия для вашего приложения/аккаунта разработчика Google Play.

Эти меры применяются ко всем регионам, если не указано иное. Например, если ваше приложение заблокировано, то оно будет недоступно во всех регионах. Чтобы меры перестали действовать, нужно подать апелляцию и дождаться ее одобрения (если не указано иное).

Отклонение

- Новое приложение или обновление не будет опубликовано в Google Play.
- Если новая версия приложения отклонена, предыдущая успешно опубликованная вами версия по-прежнему будет доступна в Google Play.
- Вы сохраните доступ к статистике, оценкам и данным о количестве установок отклоненного приложения.
- Репутация вашего аккаунта разработчика Google Play не пострадает.

Примечание. Не пытайтесь опубликовать отклоненное приложение заново, пока не устраните нарушения.

Удаление

- Приложение, а также все предыдущие его версии будут удалены из Google Play. Пользователи больше не смогут его скачать.
- Поскольку приложение будет удалено, пользователи не смогут просматривать его страницу в Google Play. Информация будет восстановлена, если вы загрузите версию, которая соответствует правилам.
- Пользователи могут потерять возможность делать покупки в приложении и использовать другие платежные функции, пока новая версия, отвечающая всем требованиям, не будет одобрена Google Play.
- Удаление не скажется на репутации вашего аккаунта разработчика Google Play. Однако если удалений несколько, аккаунт может быть заблокирован.

Примечание. Не пытайтесь опубликовать удаленное предложение заново, пока не устраните нарушения.

Блокировка

- Приложение, а также все предыдущие его версии будут удалены из Google Play. Пользователи больше не смогут его скачать.
- К блокировке могут привести серьезные и систематические нарушения правил, а также повторные отклонения и удаления приложения.
- Пользователи не смогут просматривать страницу заблокированного приложения в Google Play.
- Вы больше не сможете использовать APK и набор App Bundle заблокированного приложения.
- Пользователи потеряют возможность делать покупки в приложении и использовать другие платежные функции в нем.
- Блокировка рассматривается как предупреждение, которое сказывается на репутации вашего аккаунта разработчика Google Play. После нескольких предупреждений личный аккаунт, а также связанные с ним аккаунты разработчика Google Play могут быть удалены.

Ограничение видимости

- Видимость вашего приложения в Google Play будет ограничена. При этом оно останется доступно по прямой ссылке на страницу приложения в Google Play.
- Ограничение видимости не повлияет на репутацию вашего аккаунта разработчика Google Play.
- Пользователи по-прежнему смогут просматривать страницу приложения в Google Play.

Ограничение по региону

- Ваше приложение доступно только пользователям Google Play из определенных регионов.
- Остальные просто не смогут его найти.
- Пользователи, которые ранее установили приложение, смогут продолжать использовать его на своем устройстве, но не скачивать обновления.
- Ограничение по региону не влияет на репутацию вашего аккаунта разработчика Google Play.

Наложение ограничений на аккаунт

- Наложив ограничения на ваш аккаунт разработчика, мы удалим из Google Play все приложения в вашем каталоге и запретим вам публиковать новые или существующие приложения. У вас останется доступ к Play Console.
- Пользователи не смогут просматривать страницы удаленных приложений в Google Play и ваш профиль разработчика.
- Пользователи потеряют возможность делать покупки в приложении и использовать другие платежные функции.
- Вы по-прежнему сможете использовать Play Console, чтобы предоставлять Google Play дополнительную информацию и изменять данные аккаунта.
- Вы сможете заново опубликовать приложения после того, как устраните все нарушения правил.

Прекращение действия аккаунта

- Удалив ваш аккаунт разработчика, мы также удалим из Google Play все приложения в вашем каталоге и запретим вам публиковать новые. Все связанные аккаунты разработчика будут заблокированы навсегда.
- Повторные блокировки или блокировки, связанные с серьезными нарушениями правил, могут привести к удалению вашего аккаунта Play Console.
- Поскольку приложения, опубликованные через этот аккаунт, будут удалены, пользователи не смогут просматривать их страницы в Google Play, а также ваш профиль разработчика.
- Пользователи потеряют возможность делать покупки в приложении и использовать другие платежные функции.

Примечание. Если вы попробуете создать другой аккаунт, он также будет заблокирован (без возврата регистрационного взноса). Не пытайтесь регистрировать новые аккаунты Play Console, если один из ваших аккаунтов заблокирован.

Неиспользуемые аккаунты

Неиспользуемыми называются аккаунты разработчиков, в которых не наблюдается никакой активности. Они не соответствуют требованиям Соглашения о распространении программных продуктов .

Аккаунты разработчиков Google Play предназначены для активной публикации и поддержки приложений. Чтобы предотвратить злоупотребление сервисом, мы закрываем аккаунты, которые не используются на постоянной основе, например для размещения и обновления приложений, просмотра статистики и управления данными для Google Play.

Если мы закроем неиспользуемый аккаунт, он станет неактивен. Вы потеряете доступ ко всем отчетам, статистике и другим сведениям в Play Console до тех пор, пока мы не восстановим аккаунт. Регистрационный сбор возвращен не будет. Мы заранее сообщим о закрытии аккаунта, используя контактную информацию, которую вы для него указали.

Если в будущем вы снова захотите публиковать приложения в Google Play, то сможете создать новый аккаунт.

Сообщение о нарушениях и дальнейшие меры

Подача апелляции

Мы восстанавливаем приложения, только если они были удалены по ошибке и не нарушали Правила программы для разработчиков и условия Соглашения о распространении программных продуктов. Если вы внимательно ознакомились с правилами и считаете, что наше решение могло быть ошибочным, обжалуйте его на этой странице, или следуя инструкциям, отправленным вам по электронной почте.

Дополнительные ресурсы

Если какие-то принудительные меры в отношении вашего приложения или оценки/комментарии пользователей вызывают у вас вопросы, попробуйте найти ответы по ссылкам ниже или свяжитесь с нами через Справочный центр. Обратите внимание, что юридическую помощь мы не оказываем. Если такая помощь вам нужна, обратитесь к юристу.

- Проверка приложений
- Как сообщить о нарушении правил
- Как обратиться в Google Play по поводу удаления приложения или блокировки аккаунта
- Предупреждения
- Как сообщить о неприемлемом приложении или комментарии
- Мое приложение было удалено из Google Play
- Блокировка аккаунта разработчика Google Play

Требования к приложению в Play Console

Для безопасности экосистемы Google Play все разработчики должны выполнять требования Play Console. Это же касается профилей, связанных с вашим аккаунтом разработчика. Проверенная информация будет видна в Google Play. Это поможет укрепить доверие пользователей к разработчикам. Подробнее о том, какие данные показываются в Google Play...

Вы можете создать личный или корпоративный аккаунт разработчика Google Play. Для успешной регистрации выберите верный тип аккаунта разработчика и пройдите необходимые проверки.

Вы должны создать корпоративный аккаунт, если предоставляете:

- Финансовые продукты и услуги, например связанные с банковскими операциями, кредитами, биржевой торговлей, инвестиционными фондами, программными криптокошельками или криптовалютными биржами. Подробнее о правилах в отношении финансовых услуг...
- Приложения для здоровья, например медицинские приложения и приложения для исследований с участием людей. Подробнее о категориях приложений для здоровья...
- Приложения, которые могут использовать класс VpnService . Подробнее о правилах в отношении приложений, использующих VPN-сервисы...
- Приложения государственных органов, например разработанные государственным учреждением или по его поручению.

Выбрав тип аккаунта, сделайте следующее:

- Предоставьте точные сведения об аккаунте разработчика, в том числе указанные ниже данные.
  - Полное имя или название и адрес.
  - Номер DUNS , если аккаунт создан для организации.
  - Контактный адрес электронной почты и номер телефона.
  - Адрес электронной почты и номер телефона разработчика, доступные в Google Play (если применимо).

- Способы оплаты (если применимо).
- Сведения о платежном профиле Google, связанном с вашим аккаунтом разработчика.

- Если аккаунт создан для организации, убедитесь, что информация в нем актуальна и соответствует данным о компании в регистре Dun & Bradstreet.

Прежде чем отправлять приложение на проверку, сделайте следующее:

- Предоставьте точные и полные сведения о приложении и его метаданные.
- Загрузите политику конфиденциальности приложения и добавьте обязательную информацию в раздел безопасности данных.
- Укажите активный тестовый аккаунт, информацию для входа в него и другие сведения, необходимые для проверки приложения, например учетные данные, QR-код и т. д.

Убедитесь, что приложение работает стабильно и корректно, а также представляет ценность для пользователей. Все его элементы, включая рекламные сети, сервисы аналитики и сторонние SDK, должны соответствовать Правилам программы для разработчиков приложений в Google Play. Если в целевую аудиторию приложения входят дети, убедитесь, что оно соответствует правилам программы "Приложения для всей семьи".

Не забывайте, что вы обязаны ознакомиться с Соглашением о распространении программных продуктов и Правилами программы для разработчиков, а также убедиться, что приложение отвечает всем требованиям.

Developer Distribution Agreement

Требуется помощь?
Попробуйте следующее:

Связаться с нами
Расскажите о своей проблеме нашим сотрудникам